Manuale sulle Misure di Sicurezza e Organizzative in ambito privacy

Redatto da:	Referente Privacy – (dott.ssa Paola Amodeo)
Data creazione:	20.05.2014
Approvato da:	Innovhub - Stazioni Sperimentali per l'industria – Azienda Speciale della C.C.I.A.A. di Milano (A.S.) – con delibera del Consiglio di Amministrazione n. 27 del 10.07.2014.
Distribuzione:	Solo uso interno
Destinatari:	Dipendenti, collaboratori, stagisti, membri degli organi
Aggiornato il:	

Sommario

INTRODUZIONE E STUTTURA DEL DOCUMENTO

La struttura del presente Documento, redatto per descrivere le modalità di adozione delle misure di sicurezza minime previste dall'art. 34 D.lgs. 196/2003, di quelle idonee previste dall'art. 31 e delle eventuali misure di sicurezza necessarie in relazione a specifici trattamenti.
Il Documento redatto dal Referente per la protezione dei dati personali dell' Azienda Speciale, di seguito denominato "Referente Privacy" (dott.ssa Paola Amodeo) ed approvato con delibera del Cda, risulta finalizzato alla corretta gestione e trattamento, in ambito organizzativo e tecnologico, del dato personale (comune, sensibile e/o giudiziario) effettuato presso **Innovhub - Stazioni Sperimentali per l'industria** (nel seguito, per brevità, "A.S.").
Per ogni approfondimento sulla metodologia interna adottata si rimanda alle specifiche policy interne adottate dall'A.S..

SCOPO E CAMPO DI APPLICAZIONE

Il presente Documento ha l'obiettivo di attestare la conformità delle misure organizzative e di sicurezza a quanto stabilito dal Codice in materia di protezione dei dati personali (D.lgs. n.196 del 30 giugno 2003) e dal Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al D.lgs. n.196 del 30 giugno 2003), nonché fornire indicazioni relative alla produzione, gestione, conservazione e trasmissione delle informazioni aziendali con particolare attenzione a quelle di tipo elettronico che, per loro natura, risultano particolarmente critiche.
In questo Manuale sono altresì individuati i trattamenti, direttamente o attraverso collaborazioni esterne ovvero funzioni accentrate, effettuati da A.S., in quanto titolare (o, a seconda dei casi, co-titolare del trattamento), con l'indicazione della natura dei dati e della struttura (ufficio, funzione, etc.) interna od esterna operativamente preposta, nonché degli strumenti elettronici impiegati.
Si individuano i sistemi informativi impiegati, le precauzioni di tipo tecnologico per garantire la protezione degli strumenti elettronici e il personale coinvolto per tipologia per tutti i livelli prescritti, nonché i disciplinari cui sono assoggettati i vari soggetti coinvolti nei trattamenti.

I soggetti, a vario titolo, a cui il presente Documento fa riferimento sono:

- il **Titolare**: l'A.S., in persona del suo legale rappresentante pro tempore che, nel complesso, esercita un potere decisionale autonomo sulle finalità e modalità di trattamento dei dati personali, ivi compreso il profilo della sicurezza.

- i **Dipendenti**: dipendenti , collaboratori e stagisti dell'A.S.. Pertanto, laddove, qui di seguito, sia utilizzato il termine "Dipendenti", quest'ultimo è comprensivo anche dei collaboratori e degli stagisti.

- i **Destinatari:** Dipendenti e membri degli organi.

- gli **Interessati**: le persone fisiche cui si riferiscono i dati personali ai sensi dell'art. 4 del D.Lgs. 196/03.

- i **Responsabili**: i soggetti nominati tali dal Titolare ai sensi dell'art. 29 del D.lgs. 196/2003.

- gli **Incaricati:** i soggetti nominati tali dal Titolare o dal Responsabile di area ai sensi dell'art. 30 del D.lgs. 196/2003.

- gli **Amministratori di sistema:** figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. Vengono però considerate tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli

amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi (Provvedimento del Garante per la protezione dei dati personali del 27 Novembre 2008).
Tali soggetti per l'A.S. sono: Digicamere Scarl, InfoCamere, il dott. Marco Frittoli (amministratore di sistema interno) e il dott. Davide Cantù (amministratore di sistema interno).

RIFERIMENTI NORMATIVI E DOCUMENTALI

Il presente Documento è stato redatto in conformità a quanto previsto dalla normativa nazionale in vigore ed in particolare in conformità a quanto statuito dall'art. 34 e dall'Allegato B del Decreto Legislativo n. 196/2003 "Codice in materia di protezione dei dati personali". Si riportano, di seguito, i principali riferimenti normativi e documenti interni.

NORMATIVA ITALIANA

- **Decreto Legislativo 30 giugno 2003, n. 196** e successivi provvedimenti emanati dal Garante per la protezione dei dati personali e Allegato B (Disciplinare Tecnico in materia di misure minime di sicurezza)

- **Decreto Legislativo 8 giugno 2001, n. 231,** recante la "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'art. 11 della legge 29 settembre 2000, n. 300", pubblicato in Gazzetta Ufficiale n. 140 del 19 giugno 2001, e successive modificazioni e integrazioni.

- **Provvedimenti dell'Autorità Garante per la protezione dei dati personali**
  - Provvedimento del Garante Privacy del 27 novembre 2008 e successive modificazioni relativo a "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema"
  - Provvedimento del Garante Privacy del 13 ottobre 2008 "Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali"
  - Provvedimento del Garante Privacy del 4 luglio 2013 "Linee guida in materia di attività promozionale e contrasto allo spam"

DOCUMENTI INTERNI

Organigramma privacy A.S.
Information Security Policy
Nomine a incaricati, responsabili e amministratori di sistema (interni ed esterni)
Norme generali di comportamento - Linee Guida per l'utilizzo dei sistemi e dei servizi informatici aziendali e per il trattamento dei dati derivanti dall'utilizzo di Internet e della posta elettronica
Misure di sicurezza informatiche adottate da DigiCamere Scarl
Capitolato tecnico d'appalto del fornitore esterno PRESENT SpA
Check list amministratori di sistema
Informativa ai Dipendenti

1. STRUTTURA ORGANIZZATIVA A SUPPORTO DELLA PRIVACY

Innovhub - Stazioni Sperimentali per l'industria (di seguito denominata "A.S."), azienda speciale istituita dalla CCIAA di Milano, opera come centro di promozione dell'innovazione, dello sviluppo scientifico e tecnologico a sostegno del tessuto economico e della pubblica amministrazione e si configura come centro di ricerca dedicato alle esigenze delle imprese dei settori contribuenti afferenti alle industrie tessili, cartarie, dei combustibili, degli oli e dei grassi.
L'Azienda si articola in cinque divisioni dotate di attrezzature moderne e laboratori altamente specializzati:

- Carta
- Combustibili
- Innovazione
- Oli e Grassi
- Seta

I principali settori industriali per cui opera sono:

- filiera cartaria
- industria trasformatrice della carta
- combustibili tradizionali (petrolio, carbone, gas) e principali prodotti derivati
- combustibili alternativi (biocombustibili, combustibili da rifiuti, biomasse)
- semi e frutti oleaginosi, oli e grassi vegetali e animali e derivati
- oli minerali e lubrificanti
- detersivi e tensioattivi
- pitture e vernici
- prodotti cosmetici e di igiene personale
- fibre, filati, tessuti serici: naturali e sintetici
- filiera tessile e abbigliamento-moda

Le attività principali svolte dall'A.S. sono:
INNOVAZIONE DI PROCESSO E PRODOTTO

- Scouting di bisogni, idee, innovazioni e tecnologie
- Assistenza tecnica e consulenza alle aziende e agli enti pubblici in materia di:
    - tematiche ambientali
    - qualità o sicurezza
    - certificazione di prodotto
    - proprietà intellettuale
- Servizi di analisi, prove e controlli su materie prime, intermedi di lavorazione, prodotti finiti
- Servizi di supporto allo sviluppo di nuovi prodotti
- Servizi di progettazione/supporto al miglioramento delle tecnologie e dei processi produttivi
- Supporto nell'individuazione di partner tecnologici, laboratori di ricerca e test
- Realizzazione di progetti di ricerca scientifica - industriale e sperimentale - nei propri laboratori, con aziende e università

FINANZIAMENTI E BANDI

- Informazioni, anche tramite newsletter, sui finanziamenti e bandi comunitari, nazionali e regionali
- Supporto alle imprese per la partecipazione ai bandi tramite l'analisi dei progetti di investimento, la selezione di opportunità di finanziamento appropriate e la redazione della domanda di contributo
- Creazione di partenariati per la partecipazione a bandi comunitari, nazionali e regionali
- Coordinamento e rendicontazione delle attività progettuali

PROMOZIONE DELL'INNOVAZIONE e INFORMAZIONE

- Supporto nella partecipazione a fiere, nella realizzazione di brokerage event e nella partecipazione a social networks e ad altri strumenti di networking
- Pubblicazione di riviste e documentazione tecnico-scientifica e di dati statistici di settore
- Informazione e assistenza sulle tematiche europee
- Organizzazione di convegni, seminari, eventi

FORMAZIONE

- Organizzazione di eventi di aggiornamento e di networking

NORMAZIONE

- L'attività di normazione tecnica costituisce un compito istituzionale nei settori industriali di riferimento in ambito nazionale, europeo e internazionale. Tale attività prevede:
    - la partecipazione e il coordinamento di Gruppi di Lavoro e Commissioni per la revisione e stesura di norme tecniche;
    - lo sviluppo di metodi di prova e la predisposizione ed elaborazione della documentazione tecnica;
    - la definizione delle caratteristiche merceologiche dei prodotti delle industrie afferenti ai vari settori.

Molti dei servizi vengono erogati all'utenza attraverso un Portale, accessibile agli utenti al seguente nome di dominio:
http://www.innovhub-ssi.it.

L'A.S., per erogare i suoi servizi all'utente e per la gestione delle attività, si avvale di partner tecnologici che offrono supporto all'intero sistema camerale (es. DigiCamere, InfoCamere).
Nel presente Manuale e negli allegati è possibile verificare l'elenco completo dei soggetti terzi, la titolarità e i trattamenti sviluppati per i partner strategici che trattano dati personali di titolarità della A.S. o che offrono servizi IT a supporto dei processi e per finalità correlate alla fornitura di servizi istituzionali dell'A.S..

Presso ogni funzione della A.S., le risorse, mediante "Responsabili" o "Incaricati" (ognuno nell'ambito dell'attività lavorativa), effettuano il trattamento di dati personali di rispettiva competenza attenendosi, scrupolosamente, alle istruzioni ricevute, alle singole policy aziendali adottate ed ogni altra ulteriore indicazione, anche verbale, fornita dal Responsabile per la protezione dei dati personali di area o per il tramite dal Referente Privacy.

L'A.S., oltre al trattamento dei dati personali di cui è titolare (in maniera autonoma), può eseguire trattamenti di dati personali di titolarità di terzi soggetti giuridici (in particolare della CCIAA di Milano, delle altre Aziende Speciali o di eventuali altri soggetti del sistema camerale) con i quali vengono condivisi ed erogati servizi all'utenza (es. servizi di newsletter periodica contenente comunicazioni istituzionali o mediante le c.d. "funzioni accentrate o di staff", strutture a composizione mista che forniscono supporto alle Aziende Speciali o eventualmente ad altri soggetti del sistema camerale in diversi settori organizzativi interni); per tali motivi, alle volte l'A.S. può rivestire il ruolo di co-titolare di determinati trattamenti.
In tali casi l'A.S. è tenuta ad adottare tutte le misure per garantire la sicurezza delle informazioni e dei dati trattati oppure le misure espressamente richieste dalla CCIAA di Milano, con riferimento ai trattamenti di cui è contrattualmente responsabile, e in ogni caso nel rispetto di quanto previsto dal Codice Privacy.

In sintesi il trattamento sui dati, operato dall'A.S. può essere schematizzato identificando e classificando l'ambito del trattamento dei dati personali nel modo seguente:

1. L'A.S. tratta dati personali nell'ambito dei suoi processi interni aziendali (così come riportato nell'organigramma privacy dell'A.S.), anche attraverso il sito web sopra indicato:
    a. I trattamenti sono effettuati all'interno dell'A.S.;

b. I trattamenti sono effettuati mediante l'ausilio di "funzioni accentrate" (Risorse Umane e Organizzazione, Ufficio Acquisti, Servizio Contabilità e bilancio, Controllo di Gestione).

2. L'A.S. tratta dati personali di titolarità di terzi soggetti giuridici operanti nel sistema camerale conformemente a quanto previsto da accordi sottoscritti. In questi casi, i trattamenti sono effettuati dall'A.S. in qualità di titolare autonomo o co-titolare, direttamente nei confronti dei soggetti interessati (utenti).

L'A.S. per alcune delle attività prestate può avvalersi dell'attività (ulteriori) di fornitori esterni designati Responsabili in outsourcing del trattamento (gestione piattaforme informatiche, sito web, etc.), i quali, a loro volta, potrebbero aver bisogno di sub-appaltare determinati servizi (attività di manutenzione, hosting etc.). In tali casi, al fine di non contravvenire al principio in base al quale un responsabile non può nominare a sua volta un altro responsabile, i Responsabili nominati dall'A.S. sottoscrivono con i propri terzi fornitori (sub-appaltatori) un accordo scritto che impone a questi ultimi il rispetto degli stessi obblighi a cui il Responsabile si è vincolato in virtù della designazione ricevuta dall'A.S. e concernente il rispetto delle misure di sicurezza e di riservatezza in ambito privacy. A tal fine, come da politica aziendale, il Responsabile comunica all'A.S. (titolare del trattamento) copia dei contratti conclusi con gli eventuali terzi fornitori esterni, portando a conoscenza le principali modalità di esecuzione dei servizi resi anche dal terzo fornitore esterno (in particolare, le specifiche funzioni a cui è addetto, le tipologie di dati a cui hanno avuto accesso e le procedure adottate per garantire la sicurezza dei dati trattati).

In allegato l'organigramma privacy della A.S. (Vd. Allegato 1).

2. TRATTAMENTO DEI DATI PERSONALI DELL'A.S.

L'A.S. tratta dati personali nell'ambito della propria attività istituzionale e promozionale dei servizi sopra indicati. I trattamenti sono eseguiti mediante operazioni elettroniche attraverso il sistema informativo dell'A.S. ed il proprio sito web, nonché mediante operazioni manuali e cartacee. Tali operazioni di trattamento sono eseguite da coloro che operano in qualità di Responsabili o Incaricati dell'A.S. e da parte di soggetti esterni nominati dalla stessa Responsabili del trattamento in outsourcing.
Ciascun Responsabile deve valutare le eventuali misure di sicurezza da adottare per la propria Divisione/Funzione/Area anche in relazione alle particolari funzioni svolte e informare prontamente il Titolare e il Referente Privacy (dell'Area Risorse Umane e Organizzazione Aziende Speciali e Società Controllate) di ogni questione rilevante ai fini degli adempimenti e gli obblighi del D.lgs. 196/2003.

Struttura di riferimento: nel seguito è indicata la struttura (ufficio, funzione, etc.) all'interno della quale è effettuato il trattamento di dati personali dell'A.S., le Aree e gli Uffici, coordinati da persone espressamente nominate Responsabili dei relativi trattamenti di dati personali:

AREE DI STAFF

- **Area Affari Generali** svolge attività di supporto alla Direzione Generale, agendo come snodo tra questa, le aree aziendali, l'Ente Camerale e gli altri soggetti esterni (Responsabile art. 29 D.lgs. 196/2003 Direttore Generale, Attilio Martinetti);

- **Area Servizi Tecnici** svolge una serie di attività inerenti centralino e portierato, fattorinaggio, magazzino (in stretta collaborazione con l'Ufficio Acquisti e l'Area Amministrazione Finanza e Controllo); archivio; interventi di manutenzione, la logistica delle sedi di lavoro; smaltimento dei rifiuti speciali, condizioni di alcuni strumenti (Responsabile art. 29 D.lgs. 196/2003 Pasquale Scutifero);

- **Area Programmazione, Strategia e Comunicazione** si occupa di promuovere e coordinare le azioni delle differenti Divisioni in funzione del raggiungimento degli obiettivi aziendali; la Comunicazione opera per consolidare l'immagine aziendale unica e coordinare iniziative ed attività sia sul fronte interno che esterno (Responsabile art. 29 D.lgs. 196/2003 Direttore Generale, Attilio Martinetti);

- **Area Raccordo Qualità** svolge attività di raccordo e coordinamento dei Referenti Qualità delle singole Divisioni ed opera per assicurare il corretto funzionamento del Sistema Qualità aziendale; gestisce e mantiene i contatti con l'Ente di accreditamento; agisce in raccordo e coordinamento con Responsabili di Laboratorio, Responsabili e Responsabili Aree di Staff (Responsabile art. 29 D.lgs. 196/2003, Direttore Generale, Attilio Martinetti);

- **Area Amministrazione, Finanza e Controllo** si occupa principalmente di ottemperare agli obblighi di legge inerenti la contabilità e al bilancio. Provvede inoltre a sistematizzare determinate variabili economiche e procede ad omogeneizzarle secondo criteri unici di gestione e provvede a progettare, implementare e ottimizzare soluzioni ad elevato impatto sulla funzione amministrativa (Responsabile art. 29 D.lgs. 196/2003 Antonella Rotunno);

- **Area Acquisti** si occupa di garantire, nel rispetto delle direttive del servizio Economato CCIAA, gli acquisti di forniture, servizi, lavori di stretta pertinenza dell'AS avvalendosi dell'Ufficio Acquisti AS; (Responsabile art. 29 D.lgs. 196/2003, Eleonora Gonella);

- Area Servizio Sicurezza Salute e Ambiente si occupa di adempiere alle funzioni previste dal D.lgs. 81/2008 vale a dire assistere il datore di lavoro per valutare i rischi ed individuare le misure per la sicurezza degli ambienti di lavoro ed elaborare procedure di sicurezza per le varie attività aziendali (Responsabile art. 29 D.lgs. 196/2003, Angelo Lunghi);

FUNZIONE DI LINEA

- Funzione di Linea Servizio Marketing e Vendite ha il compito di lavorare trasversalmente in raccordo e coordinamento con le diverse Divisioni produttive, tramite un atteggiamento di orientamento al mercato e sviluppando le azioni di Marketing Strategico e Operativo (Responsabile art. 29 D.lgs. 196/2003, Direttore Generale, Attilio Martinetti);

DIVISIONI

- **Divisione Innovazione** si occupa principalmente di favorire e stimolare l'innovazione nell'imprese; eroga servizi di informazione, assistenza e supporto affiancando le imprese nello sviluppo di percorsi innovativi (Responsabile art. 29 D.lgs. 196/2003, Direttore Generale, Attilio Martinetti);

- **Divisione Oli e Grassi** offre servizi di analisi e prove, ricerca applicata, assistenza tecnica e consulenza; documentazione e informazione; formazione; certificazione di prodotti e processi produttivi, normazione nazionali ed internazionali. Svolge attività nei seguenti settori industriali: semi e frutti oleaginosi, oli e grassi vegetali e animali e derivati (proteine vegetali, lecitine, ecc.); oli minerali e lubrificanti; detersivi e tensioattivi; pitture e vernici; prodotti cosmetici e di igiene personale (Responsabile art. 29 D.lgs. 196/2003, Marco Surdi);

- **Divisione Combustibili** si occupa principalmente di effettua attività di: analisi e consulenze sui combustibili; interventi/controlli in campo ambientale e motoristico; studi e ricerca, sperimentazione, finalizzata alla soluzione di problemi specifici; normazione tecnica, assistendo enti ed aziende contribuenti rispettivamente nell'emissione e nel rispetto delle norme necessarie; supporto e consulenza alle imprese, alle pubbliche amministrazioni ed enti pubblici; promozione ed attuazione di iniziative di interesse nazionale; informazione e divulgazione scientifica (Responsabile art. 29 D.lgs. 196/2003, Angelo Lunghi);

- **Divisione Carta** si occupa di servizi di analisi; assistenza tecnica e certificazione; ricerca applicata; consulenza tecnico-scientifica principalmente nei settori carta, cartone e paste per carta e correlati (Responsabile art. 29 D.lgs. 196/2003, Patrizia Sadocco);

- **Divisione Seta** svolge, operando per il settore tessile, attività di analisi; assistenza tecnica e certificazione; ricerca applicata; consulenza tecnico-scientifica occupandosi caratterizzazione tessile, analisi termica, gestione analisi; biotecnologie e biopolimeri; ambiente e colore; Fibre; microscopia; nanotecnologie (Responsabile art. 29 D.lgs. 196/2003, Silvio Faragò);

- **FUNZIONI ACCENTRATE**: si occupano della gestione di determinate attività aziendali e svolgono attività trasversali alle Aziende Speciali della CCIAA di Milano; sono state istituite con le Disposizioni Organizzative n. 7/2012 e n. 12/2012 della CCIAA di Milano relative all'accentramento di alcune funzioni camerali.
Si tratta in particolare delle seguenti Funzioni:

- **Risorse Umane e Organizzazione Aziende Speciali e Società Controllate** (Paola Amodeo, Responsabile del trattamento e Referente Privacy)
- **Ufficio Acquisti Aziende Speciali** (Oihane Barrio, Responsabile del trattamento)
- **Controllo di Gestione Aziende Speciali** (Erika Vimercati, Responsabile del trattamento)

Poiché tali Funzioni Accentrate sono composte da personale facente parte di diversi soggetti del sistema camerale (Aziende Speciali e altri soggetti del sistema camerale), ogni Titolare provvederà – in conformità all'Accordo di riservatezza e privacy sottoscritto – a nominare i propri Dipendenti quali Incaricati ex art. 30 o Responsabili ex art. 29 D.lgs. 196/2003.

2.1. Strumentazione in generale

L'A.S. procede al trattamento di dati personali comuni, sensibili e giudiziari. Tali dati sono trattati con l'ausilio di strumenti informatici. Per strumentazione si intende l'insieme di hardware e software messo a disposizione dei Dipendenti per le sole finalità lavorative.
Tale strumentazione dovrà essere utilizzata e conservata appropriatamente per preservarne l'integrità, la disponibilità e la riservatezza delle informazioni.
Rientrano nella definizione di strumentazione i personal computer (fissi o laptop), i telefoni cellulari, i tablet, gli smartphone messi a disposizione o utilizzati dal personale.
I software presenti in azienda (comprese le postazioni dei pc) sono gestiti da Digicamere, previa richiesta della A.S. e secondo indicazioni fornite dalla stessa (relativamente all'accesso ai file server, eventuale intranet, etc.). PRESENT SpA, invece, mantiene un elenco, da aggiornare con cadenza annuale, di tutte le attrezzature informatiche di cui si serve l'A.S. per l'espletamento delle proprie attività, dello scopo cui sono destinate, della loro allocazione fisica, delle misure di sicurezza su di esse adottate e delle eventuali misure di adeguamento pianificate.

3. ELENCO DEI TRATTAMENTI

In questa sezione sono individuati i trattamenti effettuati, direttamente o attraverso condivisione esterna, dall'A.S., in quanto titolare (o co-titolare), con l'indicazione della natura dei dati e della struttura (ufficio, funzione, ecc.) interna od esterna operativamente preposta, nonché degli strumenti elettronici impiegati.

3.1. Natura dei dati trattati

Natura dei dati trattati: i dati trattati sono dati personali "comuni" e in taluni casi anche dati "sensibili" o "giudiziari", con riferimento - a titolo esemplificativo e non esaustivo - alla gestione ordinaria del rapporto di lavoro, alla gestione delle gare d'appalto o alla gestione delle controversie. La descrizione completa dei trattamenti interni e/o esterni e della natura dei dati effettuata dall'A.S. è riportata nell'Allegato 2 denominato "Catalogo dei trattamenti".
I trattamenti sono effettuati per le seguenti finalità:

- erogazione servizi di assistenza tecnica e consulenza (servizi di analisi, prove e controlli su materie prime, intermedi di lavorazione, prodotti finiti, servizi di supporto allo sviluppo di nuovi prodotti e al miglioramento delle tecnologie e dei processi produttivi) alle aziende, agli enti pubblici e ai soggetti privati;
- supporto nell'individuazione di partner tecnologici, laboratori di ricerca e test;
- realizzazione di progetti di ricerca scientifica - industriale e sperimentale - nei propri laboratori, con aziende e università;
- pubblicazione di riviste e documentazione tecnico-scientifica e di dati statistici di settore;
- erogazione servizi di informazione sulle tematiche europee (invio di informazioni, anche tramite newsletter, di aggiornamento sulle tematiche europee, sui i finanziamenti e bandi comunitari, nazionali e regionali e su iniziative correlate all'innovazione)

- supporto alle imprese per la partecipazione ai bandi tramite l'analisi dei progetti di investimento, la selezione di opportunità di finanziamento appropriate e la redazione della domanda di contributo;
- creazione di partenariati per la partecipazione a bandi comunitari, nazionali e regionali e progetti;
- coordinamento e rendicontazione delle attività progettuali;
- supporto nella partecipazione a fiere, nella realizzazione di brokerage event e nella partecipazione a social networks e ad altri strumenti di networking;
- organizzazione di convegni, seminari, eventi di aggiornamento e di networking;
- formazione tecnica e professionale nei settori industriali di riferimento tramite organizzazione di corsi di base, stage formativi e corsi specialistici, nonché mobilità di personale qualificato tra aziende e gruppi di ricerca;
- attività di normazione tecnica mediante la partecipazione e il coordinamento di gruppi di lavoro e commissioni per la revisione e stesura di norme tecniche, lo sviluppo di metodi di prova , la predisposizione ed elaborazione della documentazione tecnica e la definizione delle caratteristiche merceologiche dei prodotti delle industrie afferenti ai vari settori.
- adempimento agli obblighi di fonte legislativa, nazionale o comunitaria, regolamentare o derivante da atti amministrativi;
- esecuzione di specifici obblighi contrattuali;
- rilevazione del grado di soddisfazione della clientela sulla qualità dei servizi resi e sull'attività svolta o per attività statistiche ad uso interno;
- valutazione candidature (curriculum vitae/profili professionali);
- elaborazione buste paga e gestione contratti di lavoro;
- fatturazione dei servizi resi e finalità Amministrativo – Contabili;
- elaborazione candidature e predisposizione documenti per partecipazione a bandi e gare.

L'A.S., sulla base di una prima ricognizione, salvo apportare successive integrazioni o correzioni, dichiara di trattare i dati qui di seguito elencati:

a) dati comuni
Dato personale comune è da intendersi qualunque informazione relativa alla persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

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

c) dati giudiziari
Dati giudiziari sono quei dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, 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.

Si elencano, nell'Allegato 2 "Catalogo Trattamenti", le categorie di dati che possono essere trattati e il relativo codice di trattamento in relazione a ciascuna funzione aziendale.

3.2. Co-titolarità tra CCIAA, Aziende Speciali e altri soggetti del sistema camerale

Da alcuni anni la C.C.I.A.A. di Milano ha intrapreso un percorso finalizzato a massimizzare l'efficienza interna, attraverso la realizzazione di una serie di interventi, tra cui l'accentramento di alcune funzioni di staff, con il coinvolgimento anche delle Aziende Speciali e di altri soggetti del sistema camerale, al fine di accrescere la coerenza dell'intero sistema camerale milanese e di assicurare, pur nel rispetto delle autonomie, la condivisione di principi di gestione, regole e modalità operative.

Tale intervento organizzativo, formalizzato con le Disposizioni Organizzative della CCIAA di Milano n.7/12 e n.12/12, permette di gestire le risorse con maggiore flessibilità, secondo le esigenze dettate dai picchi di lavoro e dalle competenze presenti, di condividere le conoscenze e di incrementare la trasparenza, nonché di effettuare una lettura omogenea dei fenomeni, ottenendo evidenti economie di scala, derivanti dalla razionalizzazione delle risorse umane, strumentali e informatiche utilizzate, nonché un miglioramento della qualità del servizio reso.
Si tratta di attività che vengono svolte in maniera trasversale nei confronti delle Aziende Speciali e di altri soggetti del sistema camerale in modo accentrato, da team di lavoro "misti", ai fini di una corretta gestione e trattamento, in ambito organizzativo e tecnologico, del dato personale, per le quali è stato previsto uno specifico accordo di riservatezza per garantire l'adozione di specifici livelli di sicurezza ed evitare l'accesso ai dati da parte di soggetti non autorizzati.

E' in previsione, altresì, un sistema di gestione condivisa di dati e informazioni contenuti nei data base della CCIAA di Milano, delle Aziende Speciali ed eventualmente di altri soggetti del sistema camerale, normato attraverso l'approvazione di uno specifico Regolamento camerale nella logica di una ampia condivisione di informazioni.
Tale trattamento, sviluppato all'interno del sistema camerale (CCIAA di Milano, Aziende Speciali ed eventuali altri soggetti del sistema camerale) comprenderà:
- Strategie di comunicazione
- Raccolta e Gestione dati e contatti (Portali e Siti, Register Unico - DB unificato degli utenti iscritti ai siti -, conoscenza delle fonti informative, dei loro contenuti - forza e debolezza - e delle modalità per integrarle, etc.;)
- Analisi e Profilazione utenti (analisi e conoscenza dei comportamenti degli utenti, newsletter, strumenti di marketing operativo)
- Utilizzo degli opportuni canali di comunicazione (Portale, Siti, Newsletter, SocialNetwork, e loro utilizzo coordinato)
- Rispetto della privacy (in termini di ruoli e responsabilità, introduzione del Register Unico, regolamento interno privacy, codice di comportamento verso gli utenti e accordi scritti tra CCIAA di Milano, Aziende Speciali ed eventualmente altri soggetti del sistema camerale).
Tali trattamenti hanno come base giuridica l'art. 7 del CAD ("Qualità dei servizi resi e soddisfazione dell'utenza") e l'art. 50, comma 1 ("Disponibilità dei dati delle pubbliche amministrazioni"), in base al quale "*i dati delle pubbliche amministrazioni sono formati, raccolti, conservati, resi disponibili e accessibili con l'uso delle tecnologie dell'informazione e della comunicazione che ne consentano la fruizione e riutilizzazione, alle condizioni fissate dall'ordinamento, da parte delle altre pubbliche amministrazioni e dai privati*" e derivano dalla necessità di condividere, aggiornare e rettificare i data base della CCIAA di Milano, delle Aziende Speciali ed eventualmente di altri soggetti del sistema camerale, mediante la costituzione di specifiche piattaforme informatiche, sviluppate da Digicamere S.c.a.r.l. per conto della CCIAA, finalizzate al perseguimento di tali obiettivi.

3.3. Organi

- **Consiglio d'Amministrazione**: composto da cinque membri. Predispone i piani di sviluppo dell'A.S., adotta i provvedimenti necessari per la loro realizzazione in conformità agli indirizzi stabiliti dagli Organi della Camera di Commercio di Milano e fissa i parametri di valutazione dell'efficacia e dell'efficienza dell'azione aziendale;

- **Collegio Revisori:** composto da tre membri effettivi e due supplenti, opera secondo le disposizioni di cui all'art. 73 del DPR 2/11/2005, n. 254 e ad esso fanno carico gli obblighi previsti dalle disposizioni di legge in materia;

- **Organismo di vigilanza:** composto da tre membri, ha il compito di verificare l'effettività, l'adeguatezza e l'aggiornamento del modello organizzativo 231, previsto dal Decreto legislativo 231 del 2001, che disciplina la responsabilità amministrativa degli enti per reati commessi nel loro interesse o a loro vantaggio.

3.4. Trattamento dati affidati all'esterno

In questa sezione è esposto un quadro sintetico delle attività affidate a terzi che comportano il trattamento di dati, con l'indicazione sintetica del quadro giuridico o contrattuale (nonché organizzativo e tecnico) in cui tale trasferimento si inserisce, in riferimento agli impegni assunti, anche all'esterno, per garantire la protezione dei dati stessi.

Per gli adempimenti di legge, per la gestione dei dati degli Interessati o per altre attività dell'A.S. (es. manutenzione, hosting, newsletter e gestione dei blog i etc.), infatti, alcuni dati personali vengono affidati all'esterno e/o co-gestiti con altri titolari.

Alle società o soggetti a cui si affida l'incarico si richiede conformità di trattamento alle norme minime prescritte dal D. Lgs. 196/2003 e dall'Allegato B dello stesso.

Gli stessi, infatti, si sono impegnati, mediante apposita designazione come Responsabile esterno al trattamento (o in qualità di titolare autonomo/co-titolare) dei dati degli Interessati, a:

1. adempiere agli obblighi previsti dal Codice per la protezione dei dati personali, poiché i dati che tratterà nell'espletamento dell'incarico ricevuto sono comunque dati personali;

2. trattare i dati al solo fine dell'espletamento dell'incarico ricevuto;

3. rispettare le istruzioni specifiche contenute nella lettera di nomina, conformando ad esse le procedure già eventualmente in essere;

4. relazionare annualmente sulle misure adottate e di avvertire immediatamente i referenti della A.S. in caso di situazioni anomale o di emergenza;

5. riconoscere eventualmente il diritto della A.S. a verificare periodicamente l'applicazione delle norme di sicurezza adottate;

6. attestare l'adozione delle misure minime di sicurezza previste dall'art. 34 D.lgs. 196/2003 e del disciplinare tecnico Allegato B.

Pertanto, per le eventuali violazioni di legge poste in essere nell'ambito della propria attività di competenza, rispondono direttamente e in via esclusiva tali soggetti esterni.

Trattamenti affidati all'esterno

Descrizione sintetica dell'attività esternalizzata	**Trattamenti di dati interessati**	**Soggetto esterno**	**Descrizione dei criteri e degli impegni assunti per l'adozione delle misure**
Medico del Lavoro (visite mediche)	Dati personali comuni e sensibili del personale dipendente	Rossi Gianluca	Informativa sulla Conformità del Trattamento relativa all'espletamento dell'incarico affidato.
Servizio di amministrazione di sistema in outsourcing e di sicurezza ed assistenza informatica, realizzazione e gestione di pacchetti e strumenti informatici	Possibile accesso e visione a tutti i dati personali elettronici di titolarità di A.S.	DigiCamere Scarl	Designazione ad Amministratore di Sistema e Responsabile del trattamento in outsourcing ai sensi dell'art. 29 D.lgs. 196/2003, contenente specifica Informativa sulla Conformità del Trattamento relativa all'espletamento dell'incarico affidato.
Gestione Data Center (servizio di hosting sistemi informativi) ed elaborazione buste paga e relativi adempimenti	Possibile accesso e visione a tutti i dati personali elettronici di titolarità di A.S.	InfoCamere	Designazione ad Amministratore di Sistema e Responsabile del trattamento in outsourcing ai sensi dell'art. 29 D.lgs. 196/2003, contenente specifica Informativa sulla Conformità del Trattamento relativa all'espletamento dell'incarico affidato.
Servizio di assistenza tecnica, gestione e manutenzione delle	Possibile accesso e visione a tutti i	PRESENT SpA	Ai sensi dell'art. 29 D.lgs. 196/2003, tale società è stata nominata Responsabile esterna del trattamento,

postazioni di lavoro hardware e software in dotazione presso l'A.S., nonché dello smaltimento delle attrezzature da dismettere	dati personali elettronici di titolarità di A.S.		con l'obbligo specifico di rilasciare in favore della A.S. l'attestato di conformità di cui alla regola 25 dell'Allegato "B" al Codice Privacy (relativamente agli interventi effettuati) e di adempiere a tutto quanto previsto nel provvedimento generale del Garante per le protezione dei dati personali "Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali - 13 ottobre 2008"
Servizio di Gestione CED, Assistenza programmi, Interventi e Aggiornamento	Possibile accesso e visione (compresa l'estrapolazione) di dati personali elettronici di titolarità di A.S., nonché attività di aggiornamento sistemi operativi e prodotti di sistema, back up e recovery dei dati	DUEBI di Busti Alessandra	Ai sensi dell'art. 29 D.lgs. 196/2003, tale società è stata nominata Responsabile esterna del trattamento, con l'obbligo specifico di rilasciare in favore della A.S. l'attestato di conformità di cui alla regola 25 dell'Allegato "B" al Codice Privacy (relativamente agli interventi effettuati)
Attività di consulenza fiscale e tributaria	Dati personali comuni dei clienti e fornitori	TLS –Associazione Professionale di Avvocati e Commercialisti (associato a PWC)	Informativa sulla Conformità del Trattamento relativa all'espletamento dell'incarico affidato.
Attività di supporto per certificazione spese su progetti finanziati (audit finanziari)	Dati personali comuni di fornitori e partner di progetto	Studi di consulenza e professionisti selezionati *(presenti in una short list a rotazione)*	Informativa sulla Conformità del Trattamento relativa all'espletamento dell'incarico affidato
Attività di consulenza legale e si occupano di attività giudiziarie e stragiudiziarie della A.S.	Dati personali comuni, sensibili e giudiziari	Studi Legali	Informativa sulla Conformità del Trattamento relativa all'espletamento dell'incarico affidato.

3.5. Modalità di trattamento

I dati sopra elencati sono trattati in maniera elettronica, in forma prevalentemente automatizzata, e in forma cartacea, sia per quanto riguarda i dati personali di cui l'A.S. è titolare sia per quanto attiene ai servizi resi in regime di co-titolarità.

Il trattamento dei dati avviene, quindi, mediante strumenti manuali, informatici e telematici (Informatica Personale Distribuita, Server, File Server, posta elettronica, rete locale (LAN), rete periferica (WAN) rete internet e siti web) o telefonici (anche mediante un contact center della CCIAA di Milano, ma gestito da Digicamere, che fornisce informazioni sull'attività della A.S.) con logiche strettamente correlate alle finalità perseguite nei vari casi e, comunque, in modo da garantire la sicurezza e la riservatezza dei dati stessi.

La conservazione dei dati personali di titolarità dell'A.S. varia a seconda della tipologia e natura, oltre che dalle finalità perseguite nei vari trattamenti effettuati.
In ogni caso, in specifiche informative (cartacee o telematiche) ai sensi dell'art. 13 D.lgs. 196/2003 vengono fornite agli interessati (a seconda del trattamento) tutte le informazioni circa le finalità e le modalità perseguite nei singoli casi e in relazione agli specifici servizi forniti dall'A.S..

La tabella contenuta nell'Allegato 2 "Catalogo Trattamenti", contiene la descrizione dei trattamenti - effettuati in formato cartaceo e con l'ausilio di strumenti elettronici anche ulteriori rispetto a quelli sopra indicati - identificati, ciascuno, con un codice alfanumerico per il trattamento, specificando la natura dei dati trattati, la struttura organizzativa (interna o esterna) che effettua il trattamento, la descrizione e l'ubicazione degli strumenti utilizzati.

4. GESTIONE DEGLI INCARICATI

Sono di seguito descritti sinteticamente l'organizzazione della struttura di riferimento, i compiti e le relative responsabilità, in relazione ai trattamenti effettuati dall'A.S.

4.1. Distribuzione dei compiti e delle responsabilità

Il "**Titolare del trattamento**" dei dati: Innovhub - Stazioni Sperimentali per l'industria, in persona del suo legale rappresentante pro tempore.
Il "**Referente per la protezione dei dati personali**" o "Referente Privacy", nonché responsabile del trattamento della Funzione accentrata "Risorse Umane e Organizzazione Aziende Speciali e Società controllate", dott.ssa Paola Amodeo.
Il trattamento dei dati personali viene effettuato dai Responsabili delle aree sopra individuate (Aree di Staff, Funzioni e Divisioni) e da Dipendenti a ciò espressamente incaricati. L'A.S. ha nominato specifici soggetti quali "Responsabili del trattamento dei dati" nella propria struttura (dirigenti e responsabili degli uffici Incaricati al trattamento dei dati) ai sensi dell'art. 29 D.lgs. 196/2003, in considerazione della loro esperienza, capacità ed affidabilità, tali da offrire idonea garanzia dei pieno rispetto delle disposizioni in materia di trattamento.
Periodicamente, il Dott. Attilio Martinetti, nella sua qualità di Direttore, relaziona al Referente Privacy il livello di applicazione privacy di tutte le aree dell'A.S., sulla base di un modello di domande e risposte fornito dal Referente Privacy.

L'A.S. intende mantenere aggiornato l'impianto delle responsabilità in ambito privacy e, pertanto, provvede a rendere disponibile un apposito elenco e documenti privacy presso l'ufficio del Referente Privacy, intesi a identificare le figure incaricate, ad ogni ordine e grado, al trattamento e a fornire le istruzioni con specifiche policy interne.

L'A.S. ha nominato per iscritto i Responsabili e gli Incaricati al trattamento secondo la natura e pertinenza dei dati rispettivamente trattati, nonché ha provveduto (laddove è risultato necessario) al rispettivo rinnovo e aggiornamento periodico annuale dell'individuazione dell'ambito del trattamento consentito. Tali istruzioni sono fornite, oltre che con lettera di incarico, anche attraverso la presa visione e accettazione di policy interne sulla sicurezza.

4.2. Responsabilità di processo e di gestione

L'A.S. attua una rigorosa policy di classificazione e gestione del patrimonio informativo aziendale che attribuisce ad ogni ruolo aziendale precisi compiti e responsabilità, anche in materia di trattamento dei dati.

Tutte le persone fisiche all'interno dell'A.S. sono state autorizzate a compiere operazioni di trattamento direttamente dal Referente Privacy e/o dal proprio Responsabile del trattamento di area. Con cadenza annuale viene ridefinito o aggiornato l'ambito del trattamento dei dati nei confronti degli Incaricati. Sempre con cadenza annuale vengono verificate le condizioni dei profili di autorizzazione e qualsiasi cambiamento

che comporti la modifica dell'ambito di trattamento o la tipologia dei dati trattati all'interno delle singole unità o uffici verrà tempestivamente comunicato agli Incaricati per mezzo di circolari, comunicazioni, e-mail etc..

Tutti gli Incaricati sono nominati tali per iscritto e ricevono precise istruzioni in merito alla corretta gestione e trattamento dei dati personali (anche mediante policy interne).

A seguito dell'entrata in vigore del Provvedimento del Garante del 27 novembre 2008 relativo a "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", è, altresì, comunicata una nuova informativa ex art. 13 a tutto il personale ed un elenco "Elenco degli amministratori di sistema". Tale documento viene conservato sia internamente (relativamente ai soggetti interni che ricoprono tale ruolo) sia presso le rispettive sedi delle società DigiCamere e InfoCamere (deputate a svolgere il servizio di Amministrazioni di Sistema in outsourcing) e contiene il nominativo delle persone fisiche operanti all' interno o all'esterno della A.S. le quali, in qualità di Amministratori di Sistema, possono accedere ai dati personali di titolarità della A.S.

Tutte le Aziende Speciali hanno provveduto alla designazione di un Referente Privacy (nella persona della dott.ssa Paola Amodeo – Responsabile della Funzione Accentrata Risorse Umane ed Organizzazione Aziende Speciali e Società controllate), ai sensi dell'art. 29 del D. Lgs. 196/2003, in funzione dei suoi poteri di rappresentanza anche dell'A.S. in caso di controlli, ispezioni o richiesta di informazioni da parte dell'Autorità Garante e per quanto attiene alla tematica legata al corretto trattamento dei dati personali; ciò in relazione alle specifiche attività delegate e in considerazione della esperienza, capacità ed affidabilità espresse, tale da offrire idonea garanzia del pieno rispetto delle disposizioni in materia di privacy.

Ogni Responsabile ed Incaricato dell'A.S. deve conoscere ed uniformarsi, conformemente alla formazione ricevuta, al rispetto sia di tutte le Policy aziendali sia di ogni precauzione ed attività nelle stesse contenute e, comunque, finalizzate alla corretta gestione dei dati personali trattati.

4.3. Procedura di gestione del Sistema di autenticazione e di autorizzazione

Tutti gli Incaricati, previa sottoscrizione di una informativa, sono nominati e autorizzati al trattamento dei dati (singolarmente o per classi omogenee) mediante lettera contenente specifici compiti e istruzioni; gli stessi sono autorizzati al trattamento dei dati per le sole finalità indicate dall'A.S. (per il tramite del Responsabile di area/ufficio) ed è vietato qualsiasi altro uso dei dati personali trattati che non sia in linea con l'incarico ricevuto.

Gli Incaricati sono stati formalmente edotti in merito alla circostanza che:

a) il trattamento e la conservazione dei dati deve avvenire in modo lecito e proporzionato alle funzioni aziendali, nel rispetto della riservatezza;

b) la raccolta, registrazione ed elaborazione dei dati, mediante strumento elettronico o cartaceo, deve essere limitata alle necessità aziendali;

c) è onere dell'Incaricato la correzione od aggiornamento dei dati posseduti, l'esame della pertinenza rispetto alle funzioni;

d) è onere dell'Incaricato il rispetto dei compiti specifici che gli sono stati assegnati, nonché il rispetto delle istruzioni e delle modalità operative contenute nell'atto di conferimento dell'incarico (comprese le specifiche policy e linee guida richiamate).

Al momento della formalizzazione della nomina ad Incaricato, lo stesso riceve informazioni relativamente a:

- codice identificativo e password;
- uso delle password;
- back up dei dati aziendali rilevanti;
- policy di sicurezza a cui adeguarsi.

Il codice identificativo e la password non possono essere mai associati ad altri Incaricati e vengono disattivati se inutilizzati per 6 mesi o in caso di perdita della qualità di Incaricato.

A ogni livello di Dipendente corrisponde un diverso livello di accesso alle banche dati, in base al profilo di autorizzazione assegnato e come riportato nelle relative nomine. Almeno annualmente si verificano i profili di autorizzazione dei singoli Incaricati e si procede:

a) al conferimento di una nuova lettera di incarico (in caso di variazione del profilo di autorizzazione o di nuovi trattamenti);

b) ad una lettera di conferma dell'ambito del trattamento consentito a ciascun Incaricato (in caso non intervenga alcuna variazione).

A tutti gli Incaricati destinati al trattamento di dati mediante strumento elettronico sono state conferite credenziali di autenticazione (art. 34, comma 1, lett. b), mediante ID e parola chiave, conformi alle caratteristiche indicate nell'Allegato B e con l'obbligo di modificarle al momento della consegna ed aggiornarle periodicamente. Ogni Incaricato è custode e responsabile delle proprie password.

Ogni Dipendente, nominato Incaricato dell'A.S., risponde singolarmente, anche ai sensi del D.Lgs. 196/2003, di eventuali usi impropri dei dati e delle informazioni in particolare se, dal fatto deriva un danno ovvero un vantaggio personale.

Per rendere tutti gli Incaricati del trattamento edotti dei rischi che incombono sui dati personali, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto all'attività svolta dall'A.S., delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare, l'A.S. organizza periodicamente programmi di formazione tecnica e teorica, anche in modalità e-learning (su specifica piattaforma on-line).

Sono tenuti a seguire questi programmi tutti gli Incaricati che, a vario titolo, sono chiamati ad operazioni di trattamento dei dati personali dal momento della loro assunzione e sempre in occasione di cambiamenti di mansioni o di introduzione di nuovi significativi strumenti rilevanti rispetto al trattamento stesso.

La formazione degli Incaricati avviene sia mediante la distribuzione di documenti o manuali illustrativi (es. slide), sia mediante corsi di formazione organizzati con l'ausilio di docenti interni/esterni e tratta, in maniera particolare, la tipologia di rischi che incombono sui dati, le misure di protezione previste, le responsabilità dei soggetti che effettuano il trattamento.

Il Responsabile del trattamento di Area o Divisione nominato deve adottare tutte le idonee azioni volte al mantenimento dell'informazione evitandone la diffusione indebita; come ogni Dipendente, il Responsabile risponde singolarmente, anche ai sensi del D.Lgs. 196/2003, di eventuali usi impropri dei dati e delle informazioni in particolare se, dal fatto, deriva un danno ovvero un vantaggio personale.

Al Referente Privacy, che coordina e supervisiona le Risorse Umane e l'organizzazione delle Aziende Speciali e Società controllate, di concerto con le funzioni apicali dell'A.S., gli outsourcer delle soluzioni IT (es. DigiCamere e InfoCamere) e gli amministratori di sistema interni (dott. Marco Frittoli e dott. Davide Cantù), compete l'aggiornamento e la revisione del presente Manuale (e di tutte le policy collegate in materia sicurezza), la gestione e la responsabilità "in primis" di tutto il processo organizzativo, di controllo, di monitoraggio e di adeguamento strutturale, in materia di protezione dei dati personali.

4.4. Amministratori di sistema

L'A.S. ha individuato DigiCamere e InfoCamere quali Responsabili in outsourcing anche per il servizio di amministrazione di sistema, mentre i sig.ri Marco Frittoli e Davide Cantù sono amministratori di sistema interni; a tali soggetti sono state conferite specifiche lettere di nomina che rispettano i criteri di cui all'art. 29 d.lgs. 196/2003, quali soggetti deputati a svolgere il servizio di "amministrazione di sistema", scegliendo tali soggetti per le garanzie di esperienza, capacità e affidabilità possedute.

L'elenco degli amministratori di sistema interni (persone fisiche) della A.S., con indicata l'area aziendale operativa di appartenenza è riportato all'interno di un documento "Elenco degli amministratori di sistema" è conservato presso l'A.S..
L'elenco degli amministratori di sistema (persone fisiche) di Digicamere e di Infocamere, con indicata l'area aziendale operativa di appartenenza è riportato all'interno di un documento "Elenco degli amministratori di sistema". Tale documento è conservato presso le rispettive sedi delle società indicate ed è reso disponibile su semplice richiesta in caso di eventuali accertamenti o su richiesta dei partner istituzionali/commerciali dell'A.S..
L'operato degli amministratori di sistema e il controllo circa la rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti è demandato a specifiche funzioni esterne dei soggetti nominati.
Tale attività di verifica si svolge mediante un audit interno (effettuato eventualmente anche mediante l'ausilio di consulenti esterni) sulle misure di sicurezza e organizzative adottate, documentato in apposito verbale contenente un giudizio di conformità e compliance legale; tale attività, in particolare, viene espletata attraverso la predisposizione di un'apposita check list allegata al presente Manuale (Allegato 5), costituente altresì un presidio 231/2001 e riportante un giudizio di conformità sugli adempimenti richiesti dal provvedimento del Garante Privacy. Viene altresì verificato, almeno annualmente, che le attività svolte dagli amministratori di sistema siano conformi alle mansioni attribuite mediante lettera di nomina, ivi compreso il profilo relativo alla sicurezza.

A tal fine, i soggetti esterni sopra menzionati sono dotati di un sistema che consente la registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione (client, server, apparati di sicurezza, apparati di rete etc.) e agli archivi elettronici (file, database, posta elettronica, gestionali, ERP, log etc.) effettuati da parte degli amministratori di sistema (persone fisiche).

Alle registrazioni (access log) vengono garantite caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste, ovvero per verificare eventuali abusi e/o violazioni della riservatezza dei dati da parte di amministratori di sistema.

5. MISURE DI SICUREZZA

In questa sezione sono riportate, in forma sintetica, le misure in essere e da adottare per contrastare i rischi individuati. Per misura si intende lo specifico intervento tecnico od organizzativo posto in essere (per prevenire, contrastare o ridurre gli effetti relativi ad una specifica minaccia), come pure quelle attività di verifica e controllo nel tempo, essenziali per assicurarne l'efficacia.

In relazione al trattamento dei dati personali è, quindi, costantemente in atto un procedimento di controllo e di verifica della sicurezza del sistema informatico attraverso l'utilizzo di appositi strumenti a livello di sistema, di gestione delle basi dati e di applicativo (per ulteriori specifiche far riferimento al documento dell'analisi dei rischi), effettuato anche mediante l'ausilio di soggetti terzi (es. DigiCamere, InfoCamere).

5.1. Individuazione degli attacchi

L'individuazione degli attacchi deriva da una fase di analisi della realtà aziendale, che consta nella rilevazione dello scenario di riferimento, sia per quanto riguarda l'architettura informatica, sia per l'individuazione degli eventuali trattamenti che prevedono l'impiego di archivi di tipo cartaceo. In base a quanto rilevato, le componenti soggette a rischio risultano essere:

- ✓ reti e apparati di rete;
- ✓ elaboratori e software di sistema;
- ✓ software applicativo;
- ✓ supporti informatici di memorizzazione;
- ✓ infrastrutture;

- ✓ archivi cartacei;
- ✓ archivi di Backup.

Per contenere i rischi aventi impatto negativo sulla sicurezza dei dati, ogni funzione applica quanto contenuto nelle varie Policy aziendali, nonché in ogni altra linea guida utilizzata in favore dell'azienda.

5.2. Policy di Back up

Per tramite dei suoi outsourcer (DigiCamere e InfoCamere) e degli amministratori di sistema interni, l'A.S. adotta procedure per il salvataggio dei dati al fine di garantirne il corretto e tempestivo ripristino in caso di danneggiamento o perdita di integrità dei dati.
Le policy di back up sono descritte in una policy specifica denominata "procedure di backup" elaborata e conservata presso la sede di DigiCamere Scarl.
I sistemi sono generalmente ospitati su server ad alta disponibilità che offrono una buona resilienza a situazioni di normali guasti tecnici e con dischi ridondati permettono di ripristinare la disponibilità dei dati in caso di guasto.

A tal fine vengono effettuate le seguenti operazioni:

a) esecuzione giornaliera del back up attraverso procedure automatiche;
b) report dei back up effettuati;
c) archiviazione e verifica della procedura di ripristino dai supporti di back up.

I sistemi più critici sono ospitati presso la server farm InfoCamere di Via Viserba, in locali contigui alla sede operativa di DigiCamere e possono essere ripristinati da un sito alternativo in caso di distruzione del sito primario. Il back up della posta elettronica, invece, avviene sui server di Google (vd. contratto di "Fornitura di caselle di Posta Elettronica e servizi aggiuntivi Google" sottoscritto con Noovle Srl). Con riferimento a tale procedura si rinvia ai termini di servizio di Google (https://support.google.com/a/answer/60762?hl=it), che si ritiene rappresentino una sufficiente e adeguata garanzia di salvataggio dei dati ai sensi dell'art. 34, comma 1, lett. f) del d.lgs. 196/2003.

Ogni giorno viene effettuato un salvataggio delle partizioni dati dei dischi dei sistemi. Il giorno successivo i backup vengono riversati su nastro e spostati in un centro remoto di archiviazione. Le partizioni di sistema dei server vengono riversate una volta alla settimana.

Vengono conservate 20 generazioni di backup.

Per gli altri outsourcer di cui si servono le società responsabili del back up (DigiCamere e InfoCamere), i nastri di backup sono custoditi presso le rispettive server farm e possono prevedere il deposito di una copia presso depositi remoti.

5.3. Misure di protezione

Sulla base degli attacchi individuati e delle necessità di protezione espresse dai requisiti precedentemente descritti, sono state adottate un insieme di misure di protezione così classificabili:

- ✓ **Misure di tipo organizzativo**. Rientrano in tale categoria:
  - le misure per l'assegnazione di compiti e responsabilità (nomine);
  - le misure per l'aumento della sensibilità aziendale nei confronti delle tematiche di tutela dei dati (formazione);
  - le misure per evitare l'attuazione di trattamenti di dati personali per finalità diverse da quelle autorizzate e consentite;
  - le misure per la protezione di archivi cartacei e di supporti di memorizzazione (nastri, cd/DVD ecc.).

- ✓ **Misure di protezione delle aree e dei locali (criteri di protezione fisica)** e rispettive procedure. Rientrano in tale categoria:
  - le misure per la protezione dall'accesso intenzionale e non autorizzato ai locali e agli archivi (anti-intrusione);

- le misure per la protezione dei locali dall'accesso non autorizzato (intenzionale o non intenzionale) tramite le vie di accesso predisposte (controllo accesso);
- le misure per la protezione dei dati da eventi di origine naturale o dolosa (antincendio);
- le misure per la protezione da condizioni ambientali proibitive o da eventuali riduzioni dell'efficienza dei sistemi di supporto (impianti ausiliari).

✓ **Misure di protezione delle architetture di rete, degli applicativi e delle banche dati** (criteri di protezione logica dei dati) e relative procedure. Rientrano in tale categoria:
- le misure per la protezione da accessi non autorizzati ad informazioni riservate (User-id, password, screensaver con password);
- le misure per la protezione da possibili danneggiamenti alle informazioni (antivirus);
- le misure per la protezione da eventuali perdite di disponibilità dei dati (back up completo giornaliero dei file server, mail server, application server ect.);
- le misure necessarie finalizzate alla registrazione degli access log degli amministratori di sistema in ottemperanza al provvedimento dell'Autorità Garante per la protezione dei dati personali del 27 novembre 2008 "*Misure e accorgimenti prescritti ai titolari di trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*".

✓ **Misure di protezione durante la trasmissione dei dati** e relative procedure.
Rientrano in tale categoria:
- le misure per la trasmissione sicura delle informazioni su rete;
- le misure per il trasferimento di dati mediante mezzi differenti dagli elaboratori.

La bontà delle misure adottate è periodicamente verificata secondo la seguente tabella:

Attività	**Verifiche**	**Periodicità**	**Riferimento normativo**
Individuazione dell'ambito del trattamento consentito ai singoli Incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici	A cadenza almeno annuale viene verificato l'aggiornamento periodico delle lettere di incarico e dei profili di autorizzazione	Annua	Allegato B al D. Lgs. n.196/03
Misure contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale		Giornaliera	Allegato B al D. Lgs. n.196/03
Misure volte a prevenire la vulnerabilità degli strumenti elettronici e a correggerne i difetti		Giornaliera	Allegato B al D. Lgs. n.196/03
Salvataggio dei dati	Frequenza giornaliera con procedure automatiche	Giornaliera	Allegato B al D. Lgs. n.196/03
Misure e accorgimenti, prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di Amministratore di Sistema	Controllo delle registrazioni degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici effettuati da parte degli Amministratori di Sistema e Audit Interno sullo stato di applicazione delle misure organizzative e tecniche di sicurezza	Annua	Provvedimento del Garante Privacy del 27 novembre 2008 e successive modifiche

Piano di verifica periodico delle misure adottate

Di seguito vengono descritte le misure di sicurezza atte a garantire:
- la protezione delle aree e dei locali;
- la corretta archiviazione e custodia di atti, documenti e supporti contenenti dati personali;
- la sicurezza nell'ambito dell'utilizzo degli strumenti elettronici.

Per quanto concerne il rischio d'area legato ad eventi di carattere distruttivo, gli edifici e locali nei quali si svolge il trattamento dei dati sono protetti da:

- dispositivi antincendio;
- gruppi di continuità dell'alimentazione elettrica;
- gruppo elettrogeno;
- impianto di condizionamento;
- impianto elettrico dotato di misure salvavita atte anche ed evitare cortocircuiti e possibili incendi.

Climatizzazione dei locali:

- i locali sono climatizzati, in particolare nel datacenter situato presso la sede di InfoCamere SpA e gestito da DigiCamere (es. per le attività di back up).

Per l'esatta indicazione delle misure di protezione (organizzative e di sicurezza) adottate, si rinvia alla specifiche policy e procedure interne adottate da DigiCamere (responsabile esterna del trattamento), e allegate al presente Manuale (Allegato 4). Tale documento, infatti, rappresenta una sintesi delle misure di sicurezza delle quali DigiCamere garantisce l'applicazione anche per la specifica realtà della A.S..
Per l'applicazione e descrizione delle ulteriori misure di sicurezza hardware e software si rinvia altresì all' Allegato 3 "Capitolato tecnico d'appalto" del fornitore esterno PRESENT SpA, responsabile della sicurezza informatica e garante della conformità alle norme e standard di sicurezza in ambito IT (es. ISO/IEC 27001:2005, d.lgs. 196/2003, etc.). PRESENT SpA, in particolare, mantiene un inventario aggiornato degli hardware e software forniti e installati presso l'A.S. (mediante lo strumento di Discovery di LANDESK).

Per quanto riguarda le misure atte ad impedire gli accessi non autorizzati, gli edifici ed i locali nei quali si effettua il trattamento dei dati sono protetti da:

- sistemi di allarme e di sorveglianza anti-intrusione (con registrazione dei codici di ingresso e registrazione degli eventi nel tempo);
- porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee;
- limitazioni all'accesso del data center (localizzazione del server);
- accesso controllato, mediante servizio di guardiania e portineria e tesserino magnetico abilitato;
- vigilanza che interagisce con il personale dell'A.S. o videosorveglianza;
- in ciascun ufficio sono presenti armadi, schedari e cassetti dotati di chiusura a chiave, nei quali sono custoditi documenti cartacei contenenti dati personali;
- procedura di identificazione dei visitatori.

Dispositivi antincendio (estintori, manichette, impianti di rilevazione e/o spegnimento automatico):

1. antincendio a Gas nei locali interni;
2. estintori distribuiti in tutto l'edificio.

5.4. Procedure interne volte alla gestione dei codici di identificazione

Misure minime di riferimento: *(Vd. Allegato B al D. Lgs. n.196/03 regola n° 1, 2, 3, 6,7,8)*

Il trattamento dei dati personali, con strumenti elettronici, è consentito esclusivamente agli Incaricati dotati di credenziali di autenticazione. Le credenziali di autenticazione sono individuali ed identificano univocamente l'Incaricato sui sistemi di elaborazione cui ha accesso.
Ad ogni Incaricato è associato un profilo che gli consente l'accesso ad uno o più specifici trattamenti in base alle funzioni cui egli è preposto.
È compito degli Amministratori di Sistema approntare gli strumenti ed i controlli mediante cui verificare il corretto uso delle credenziali di autenticazione, nonché monitorare e vigilare sui tentativi di accesso non autorizzato.
In caso di perdita della qualità che consente all'Incaricato l'accesso ai dati personali, si procede alla verifica del profilo (cessazione attività o cambio di ruolo).

Le credenziali di autenticazione non utilizzate da almeno 6 mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
Esiste una procedura di disattivazione delle credenziali in caso di dimissioni di un Incaricato al trattamento dei dati personali.
L'Area Risorse Umane e Organizzazione Aziende Speciali e Società controllate deve dare informazione a Digicamere circa le dimissioni del personale o lo spostamento di mansione per annullare le credenziali di autenticazione dell'Incaricato del trattamento.
Nel caso in cui un Responsabile di area della A.S. richieda una modifica rispetto alla configurazione dell'accesso al file server da parte di un Dipendente, tale richiesta va rivolta a Digicamere e per conoscenza va inviata all'Area Risorse Umane e Organizzazione Aziende Speciali e Società controllate.

5.5. Gestione, custodia e aggiornamento della parola chiave (Password)

Misure minime di riferimento: *(Vd. Allegato B al D. Lgs. n.196/03 regola n° 4,5,9)*

Tutte le stazioni di lavoro sono protette da una user name e password, così come per l'accesso ai server, che rispetta i requisiti minimi di complessità (8 caratteri alfanumerici con lettere maiuscole e minuscole) e che viene regolarmente cambiata ogni 90 giorni.

Tutte le operazioni, riguardanti la gestione delle password svolte nel sistema informativo dagli utenti, vengono registrate in un file di registro (ogni pc ha memoria dell'evento "modifica pw" per un periodo di tempo ben definito oltre il quale vengono sovrascritte; si ha traccia anche delle stesse password su domain controller, ma in entrambi i casi citati le informazioni sono crittografate e, pertanto, nessuno può accedere alle password utilizzate dall'utente).

La password di accesso presenta le seguenti caratteristiche:
a) Non corrisponde al nome utente o ai dati personali dell'utente;
b) Ha una lunghezza di almeno otto caratteri alfa-numerici;
c) Non corrisponde ad una semplice parola rintracciabile in un dizionario;
d) Non contiene riferimenti agevolmente riconducibili all'Incaricato.

Definizione delle credenziali di autenticazione, individuate tra le seguenti tipologie:
- Codice identificativo, più parola chiave;
- Il sistema principale di gestione dell'autenticazione avviene tramite l'interfaccia utente del sistema operativo tramite procedura di log-in, la sicurezza del sistema è garantita da Digicamere, che gestisce in Dominio per conto dell'A.S. (Active Directory).

Le regole per la gestione della parola chiave sono le seguenti:
- Scadenza dopo 3 mesi di utilizzo;
- Non è possibile reintrodurre la password precedente (memorizzazione delle 4 ultime chiavi);
- Almeno 8 caratteri;
- Presenza di numeri / caratteri speciali necessaria;
- Scadenza dell'account utente dopo 6 mesi di inutilizzo.

Modalità di attivazione, variazione e gestione delle password:
a) l'attivazione della parola chiave è fatta da chi si occupa dell'amministrazione del sistema e l'utente è obbligato a modificare tale parola chiave al primo utilizzo del suo account;
b) è sempre possibile la modifica in via autonoma della parola chiave da parte dell'utente;
c) è possibile forzare (resettare) la parola chiave da parte dell'amministratore di rete portando a conoscenza dell'utente la forzatura effettuata nel caso fosse necessario.

Il processo di autenticazione consente di ottenere agli Incaricati uno specifico insieme di privilegi di accesso ed utilizzo rispetto alle risorse del sistema informatico.

Gli Incaricati al trattamento dei dati, osservano le seguenti istruzioni per l'utilizzo degli strumenti informatici:
- obbligo di custodire i dispositivi di accesso agli strumenti informatici (username e password);
- obbligo di non lasciare incustodito e accessibile lo strumento elettronico assegnato durante una sessione di trattamento;
- obbligo assoluto di riservatezza;

- divieto di divulgazione della password di accesso al sistema (non solo a soggetti esterni, ma neppure a persone appartenenti all'organizzazione, siano essi colleghi, responsabili del trattamento, amministratori di sistema, etc.).

Ad ogni Incaricato è imposto l'aggiornamento periodico della password con sistema automatico.

5.6. Utilizzo delle parole chiave in caso di emergenza (assenza dell'Incaricato)

Misure minime di riferimento: *(Vd. Allegato B al D. Lgs. n.196/03 regola n° 10)*
Questa procedura è attivata in caso di urgenza di accesso ai dati di un trattamento, in assenza dell'Incaricato.

Digicamere assicura la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'Incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema; a tal fine sono impartite idonee e preventive disposizioni scritte.
Un Amministratore di Sistema di Digicamere, avvisato da un Responsabile della risorsa interessata (con in copia il Responsabile dell'area Risorse Umane e Organizzazione Aziende Speciali e Società controllate) o direttamente dall'area Risorse Umane e Organizzazione Aziende Speciali e Società controllate, può resettare la parola chiave e autorizzare l'accesso ai dati ad un ulteriore Incaricato, dando tempestiva informazione all'Incaricato non reperibile sull'intervento effettuato (rendendo quindi visibile all'utente la forzatura effettuata nel caso fosse necessario).

5.7. Sistema di assegnazione e controllo dei profili

Misure minime di riferimento: *(Vd. Allegato B al D. Lgs. n.196/03 regola n° 12,13,14)*

Ogni Incaricato ha un proprio profilo di autorizzazione e può accedere ai soli dati a lui consentiti o per semplicità di gestione amministrativa, può accedere ai soli dati consentiti alla classe omogenea di incarico alla quale appartiene (group policy). Tali profili autorizzativi sono configurati sugli appositi strumenti di sicurezza e di controllo delle autorizzazioni, delle piattaforme elaborative elettroniche.
I profili di autorizzazione, per ciascun Incaricato o per classi omogenee di Incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento. Il processo di assegnazione del profilo di autorizzazione avviene con queste modalità:

- consegna dell'informativa e delle policy sull'uso appropriato delle credenziali utente;
- creazione del profilo di autorizzazione sui sistemi;
- consegna delle credenziali e password.

In conformità a quanto disposto dal punto 4 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del D.lgs. n.196 del 30 giugno 2003), gli Incaricati debbono adottare le necessarie cautele per assicurare la segretezza della parola chiave e custodire diligentemente ogni altro dispositivo che gli è stato affidato per i sistemi di autenticazione informatica (badge magnetici, tessere magnetiche, etc.).

5.8. Misure di prevenzione da programmi dannosi o da accessi abusivi

Misure minime di riferimento: *(Vd. Allegato B al D. Lgs. n.196/03 regola n° 16,17,20)*

I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante un Sistema Antivirus aggiornato più volte al giorno, previa disponibilità degli aggiornamenti. L'aggiornamento avviene in modalità automatica. Nel caso venga riscontrata la presenza di virus informatici, si attiva una specifica procedura di gestione delle minacce.
In particolare, l'antivirus si attiva automaticamente in presenza di virus. Nel caso in cui il problema non venga neutralizzato in prima battuta, poiché può accadere che la rilevazione provenga dall'utente che - a causa del virus – ha riscontrato un problema, viene aperto uno specifico ticket. Può accadere, altresì, che PRESENT SpA rilevi un allarme del sistema e intervenga direttamente sui sistemi dell'A.S., oppure, in via residuale, può

accadere che il virus venga rilevato direttamente da Digicamere, in quanto quest'ultima ha la gestione complessiva del sistema antivirus. Quest'ultime in tali casi, procederanno all'attuazione delle proprie procedure interne e all'adozione di tutte le specifiche misure di sicurezza per risolvere il problema.
Per l'applicazione e descrizione delle ulteriori misure di sicurezza hardware e software si rinvia altresì all'Allegato 3 "Capitolato tecnico d'appalto" del fornitore esterno PRESENT SpA, responsabile della sicurezza informatica e garante della conformità alle norme e standard di sicurezza in ambito IT (es. ISO/IEC 27001:2005, d.lgs. 196/2003, etc.).

5.9. Misure a protezione dei dati sensibili degli Interessati

I dati personali comuni (ed eventualmente quelli sensibili e/o giudiziari) degli Interessati ospitati su strumenti elettronici dell'A.S. sono protetti mediante l'adozione di tecniche di cifratura e/o di anonimizzazione, nonché attraverso la distruzione dei supporti rimovibili sui quali eventualmente tali dati sono stati salvati.

La procedura di distruzione dei supporti rimovibili (apparecchiature hardware) di proprietà della A.S. avviene per il tramite della società PRESENT SpA, nel rispetto del provvedimento dell'Autorità Garante "Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali" del 13 ottobre 2008.

5.10. Archivi cartacei

Misure minime di riferimento: *(Vd. Allegato B al D. Lgs. n.196/03 regola n° 27,28,29)*

All'interno dell'A.S. vengono trattati e/o conservati i documenti che possono contenere dati personali degli Interessati. L'archivio cartaceo viene comunque gestito nel pieno rispetto delle idonee misure di sicurezza in relazione al tipo di documentazione in esso contenuta.

Gli eventuali atti e documenti contenenti dati personali sensibili e/o giudiziari sono affidati agli Incaricati del trattamento per lo svolgimento dei relativi compiti; i medesimi atti e documenti sono controllati e custoditi dagli Incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.
L'accesso agli archivi contenenti dati sensibili e/o giudiziari è controllato ed consentito solo agli incaricati a ciò espressamente autorizzati. Si precisa che l'accesso agli uffici non è consentito a soggetti esterni o al pubblico.
Quando gli archivi non sono dotati di strumenti per il controllo degli accessi, le persone che vi accedono sono preventivamente autorizzate.

La documentazione aziendale di carattere riservato o contenente dati sensibili e/o giudiziari viene conservata all'interno di armadi con serratura.
Gli archivi cartacei vengono gestiti secondo le seguenti modalità:

- possono accedere alle informazioni contenute nell'archivio cartaceo solo i Responsabili designati e gli Incaricati da questi autorizzati con lettera scritta;
- l'accesso alle informazioni è consentito limitatamente ai soli dati personali la cui conoscenza è strettamente necessaria per lo svolgimento dei compiti assegnati;
- tutti i documenti che contengono dati personali sono conservati in archivi ad accesso selezionato.

Modalità di identificazione e registrazione degli accessi ai dati particolari dopo l'orario di chiusura: non esiste un sistema di controllo degli accessi che permette di registrare tempi di ingresso dei vari Dipendenti oltre all'orario di ufficio in quanto, per policy aziendale, nessuno può accedere oltre gli orari di apertura dell'edificio. In ogni caso, vi è la presenza di guardie all'ingresso che presidiano gli accessi alla struttura.

Per i trattamenti di dati personali effettuato senza l'ausilio di strumenti elettronici, pertanto, Responsabili e Incaricati del trattamento dei dati personali sono stati istruiti per l'osservanza delle ulteriori e seguenti disposizioni:

- i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici non devono essere portati al di fuori dei locali individuati per la loro conservazione se non in casi del tutto eccezionali e, nel caso questo avvenga, l'asportazione deve essere ridotta al tempo minimo necessario per effettuare le operazioni di trattamento;
- per tutto il periodo in cui i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici sono al di fuori dei locali individuati per la loro conservazione, il Responsabile o l'Incaricato del trattamento non dovrà lasciarli mai incustoditi;
- il Responsabile o l'Incaricato del trattamento deve, inoltre, controllare che i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici, composti da numerose pagine o più raccoglitori, siano sempre completi e integri;
- al termine dell'orario di lavoro tutti i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici, devono essere riportati nei locali individuati per la loro conservazione;
- i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici non devono essere mai lasciati incustoditi nelle postazioni di lavoro durante l'orario di lavoro;
- si deve adottare ogni cautela affinché ogni persona non autorizzata non venga a conoscenza del contenuto di documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici;
- per evitare il rischio di diffusione dei dati personali trattati senza l'ausilio di strumenti elettronici, si deve limitare l'utilizzo di copie fotostatiche;
- particolare cautela deve essere adottata quando i documenti sono consegnati in originale a un altro incaricato debitamente autorizzato;
- documenti contenenti dati personali sensibili o dati che, per una qualunque ragione siano stati indicati come meritevoli di particolare attenzione, devono essere custoditi con molta cura;
- è tassativamente proibito utilizzare copie fotostatiche di documenti (anche se non perfettamente riuscite) all'esterno del luogo di lavoro.

6. PIANIFICAZIONE DEGLI INTERVENTI FORMATIVI

In questa sezione sono riportate le informazioni necessarie per individuare il quadro sintetico degli interventi formativi effettuati e che si prevede di svolgere.

In ambito sicurezza delle informazioni e Privacy, infatti, saranno predisposte sessioni formative in e-learning da fruire attraverso l'uso di internet e la relativa documentazione sarà disponibile presso la intranet aziendale. Ciò consentirà di accrescere le proprie competenze e di riflesso migliorare la gestione delle informazioni aziendali. Tutti i corsi di formazione previsti non sono facoltativi e la mancata ed ingiustificata assenza può portare a provvedimenti di tipo tecnico-disciplinare nei confronti di Incaricati e Responsabili (così come stabilito dalla Information Security Policy).

In ragione delle lettere di incarico e di nomina conferite a tutti i soggetti che trattano dati personali, per attestare le esatte istruzioni rilasciate agli incaricati, al fine di consentire di adempiere correttamente alle prescrizioni normative e per rendere quest'ultimi edotti dei rischi che incombono sui dati personali, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto all'attività svolta dall'A.S., nonché delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate, vengono periodicamente organizzati dall'area sopra individuata programmi di formazione tecnica e teorica.
Sono tenuti a seguire questi programmi tutti i Dipendenti che, a vario titolo, sono chiamati ad operazioni di trattamento dei dati personali dal momento della loro assunzione e sempre in occasione di cambiamenti di mansioni o di introduzione di nuovi significativi strumenti rilevanti rispetto al trattamento stesso o novità legislative.

Il Referente Privacy, in collaborazione con i Responsabili degli specifici trattamenti di dati personali della varie aree aziendali, valuta per ogni incaricato (o classe omogenea di incaricati) a cui è stato affidato il trattamento, sulla base dell'esperienza, delle sue conoscenze ed in funzione anche di eventuali opportunità offerte dall'evoluzione tecnologica, se è necessario pianificare interventi di formazione specifici.

La formazione dei Responsabili e Incaricati al trattamento dei dati è programmata già al momento dell'ingresso in servizio; tale formazione, oltre a fornire le competenze e gli strumenti operativi per svolgere le proprie mansioni quotidiane, fornisce le informazioni necessarie per gestire le informazioni in conformità con la legge sulla privacy e sensibilizza tali soggetti sulla corretta condotta da seguire per la salvaguardia della riservatezza dei dati.
Inoltre, la formazione è programmata in occasione di cambiamenti di mansione o introduzione di nuovi significativi strumenti o modifiche legislative, rilevanti rispetto al trattamento di dati personali.

Coerentemente con l'evoluzione degli strumenti tecnici adottati e/o dall'insorgere di nuove disposizioni legislative in materia, verranno istituiti nuovi incontri formativi. In ogni caso, periodicamente, verrà comunque istituito un incontro per sensibilizzare Responsabili e Incaricati di determinate aree aziendali sull'importanza di adottare le norme di sicurezza predisposte e per recepire eventuali suggerimenti in materia derivanti dalla constatazione della presenza di minacce o vulnerabilità riscontrate.

7. CONTATTI

I seguenti contatti seguenti saranno di aiuto nei casi sotto indicati:

Problematiche di utilizzo dei software, hardware e dispositivi informatici in genere, problematiche legate alle password e in generale di accesso ai sistemi dell'A.S., problematiche legate al proprio account e alla posta elettronica, problematiche legate alla navigazione web e ai tool aziendali:

Digicamere, tramite apertura di un "SOS Ticket" sul portale di assistenza informativa e, in via subordinata, telefonicamente al numero 8500. A seguito della segnalazione, si attiva la procedura "Procedura SOS Ticket" e, a seconda del problema segnalato, potrà essere coinvolta Digicamere Scarl o PRESENT SpA.

Per problematiche relative ad aspetti di Information Security, Compromissione di account, Disclosure di informazioni aziendali all'esterno dell'A.S. e in generale diffusione non autorizzata di dati comuni, sensibili e/o giudiziari trattati dalla A.S.:

Referente Privacy (dott.ssa Paola Amodeo) – paola.amodeo@mi.camcom.it – Telefono (Orario 9.00 – 18.00) - +39 0285155146.

Tali contatti sono utilizzabili anche per consigli relativi al miglioramento della sicurezza delle informazioni.

8. REVISIONI E ALLEGATI

Il presente documento, contenente una descrizione di tutte le procedure e misure di sicurezza di cui agli art. 31 e ss. del D.lgs. 196/2003 e dell'Allegato B viene sottoposto a revisione annuale nella sua interezza o in presenza di modifiche sostanziali nell'organizzazione e nell'adozione delle misure di sicurezza fisica e logica.

REVISIONI

N°	ATTIVITÀ	FUNZIONE	DATA	NOME

REVISIONI

N°	ATTIVITÀ	FUNZIONE	DATA	NOME
1	REDATTO DA	Referente Privacy	30.04.14	Manuale sulle Misure di Sicurezza e Organizzative in ambito privacy
2	REVISIONE			

ALLEGATI

N°	NOME	DATA	AGGIORNATO AL
1	Organigramma privacy A.S.	30.05.14	
2	Catalogo Trattamenti	30.05.14	
3	Capitolato tecnico d'appalto del fornitore esterno PRESENT SpA	12.07.12 (bando europeo n. 2012/S 132 - 219805	
4	Misure di sicurezza informatiche adottate da DigiCamere Scarl	20.02.14	
5	Check list amministratori di sistema + Elenco amministratori interni	30.05.14	