Regolamento interno in materia di privacy

CUP 2000 S.p.A.

CUP 2000 S.p.A. - Sede Legale
Via del Borgo di S. Pietro, 90/c
40126 Bologna
tel. +39 051 4208411
fax +39 051 4208511
cup2000@cup2000.it - cup2000@cert.cup2000.it - www.cup2000.it

C.F., P. IVA e Iscrizione al Registro delle Imprese di Bologna n. 04313250377 - Capitale Sociale €. 487.579,00 i.v.

Sommario

PREMESSA ... 3

AMBITO DI APPLICAZIONE DEL REGOLAMENTO ... 3

VIOLAZIONE DEL REGOLAMENTO ... 4

RINVIO ... 4

Definizioni richiamate dal Codice Privacy ... 5

1. Organigramma privacy ... 7

1.1. Titolare del trattamento ... 7

1.2. Delegato alla gestione della privacy ... 7

1.3. Funzione Affari Generali ... 7

1.4. Responsabili esterni ... 7

1.5. Amministratori di sistema ... 8

1.6. Incaricati del trattamento ... 9

1.7. Addetti alla manutenzione e gestione ... 9

1.8. Unità di trattamento ... 9

2. Regole operative ... 10

Regole generali per tutti i trattamenti ... 10

3. Misure di sicurezza ... 13

- MISURE MINIME per trattamenti effettuati con strumenti elettronici ... 13
- MISURE MINIME per trattamento di dati effettuati con atti e documenti cartacei o strumenti non elettronici ... 15

4. Istruzioni specifiche per preposti ed amministratore di sistema ... 16

INCARICATI DEL TRATTAMENTO ... 16

Modalità di svolgimento delle operazioni: (modalità specifiche che riguardano solo alcuni incaricati) ... 17

Istruzioni per l'uso degli strumenti del trattamento ... 17

Istruzioni in tema di sicurezza ... 18

AMMINISTRATORI DI SISTEMA ... 19

ADDETTI ALLA MANUTENZIONE ... 21

PREMESSA

Il presente Regolamento è emanato con atto del Direttore Generale, delegato dal Consiglio di Amministrazione alla gestione ed organizzazione della privacy interna alla società, al fine di individuare le norme comportamentali e le procedure tecnico-organizzative cui è necessario attenersi in materia di trattamento di dati personali e di sicurezza nello svolgimento di tutte le attività istituzionali CUP 2000 S.p.A.. (di seguito anche "Società")

In particolare, si ritiene necessario definire una chiara disciplina interna atta garantire che il trattamento dei dati personali svolto nell'ambito delle mansioni lavorative, avvenga - come espressamente previsto all'art. 2 del D. Lgs. 30 giugno 2003 n. 196 e s.m.i. recante "Codice in materia di protezione dei dati personali"(di seguito anche "Codice Privacy) - "*nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali*".

AMBITO DI APPLICAZIONE DEL REGOLAMENTO

– *AMBITO SOGGETTIVO*

Tutte le persone fisiche che, nell'esercizio delle proprie mansioni/attività istituzionali ed a qualsiasi titolo svolgono attività in qualità di "incaricato del trattamento dei dati personali", di "addetti alla gestione o alla manutenzione degli strumenti elettronici" e di "amministratore di sistema" e comunque tutti coloro, incluse le persone giuridiche, che trattano, in qualsiasi ruolo, dati personali e sensibili di titolarità di CUP 2000/che CUP 2000 tratta in qualità di responsabile esterno, sono tenuti al rispetto delle regole di seguito elencate.
Il presente regolamento si applica inoltre a tutti coloro che, anche mediante accesso alla rete informatica, utilizzano strumenti elettronici e soluzioni tecnologiche o usufruiscono di servizi la cui sicurezza è gestita da CUP 2000 S.p.A.

– *AMBITO OGGETTIVO*

Il regolamento si applica alle attività che comportano il trattamento dei dati personali di **titolarità di CUP 2000 S.p.A**. (quali, ad es. attività connesse alla gestione del personale, agli organi societari e agli adempimenti relativi ai propri clienti, fornitori ed eventuali consulenti, per cui la Società ha titolarità autonoma) ovvero alle attività che comportano il trattamento dei dati personali per le quali CUP 2000 S.p.A. sia stata individuata, ai sensi dell'art. 29 del Codice Privacy, in qualità di **responsabile esterno del trattamento** (quali, ad es. attività oggetto di convenzioni di servizio sottoscritte con Aziende Sanitarie ed Ospedaliere ovvero con la Regione Emilia Romagna per le quali ha ricevuto apposita nomina, eventualmente con funzioni di amministrazione di sistema) nel rispetto delle finalità determinate dai committenti e secondo le modalità previste dalla convenzione di servizio e dalla nomina ricevuta.

Le nomine di CUP 2000 s.p.a. in qualità di responsabile esterno del trattamento definiscono l'ambito del trattamento autorizzato da parte dei Soci titolari. **Nessun trattamento ulteriore è consentito**, se non previa autorizzazione dei titolari a cui

compete in via esclusiva la verifica della compatibilità dei trattamenti effettuati rispetto alle informative rilasciate ex art. 13 del Codice Privacy ed ai consensi acquisiti dagli interessati.

- *INFORMATIVE SUL TRATTAMENTO DEI DATI PERSONALI rilasciate da CUP 2000 ai sensi dell'art. 13 del Codice Privacy*

– **Dati di titolarità di CUP 2000**

Il trattamento dei dati personali e sensibili di **titolarità di CUP 2000** viene effettuato nel rispetto delle finalità e con le modalità indicate nell'informativa ai sensi dell'art. 13 del Codice Privacy preliminarmente rilasciata gli interessati ai fini dell'acquisizione del relativo consenso. L'informativa viene aggiornata periodicamente ed in ogni caso in coerenza con la validità temporale dell'Autorizzazione Generale dell'Autorità Garante per la protezione dei dati personali.

- **L'informativa al personale dipendente** viene rilasciata, ed il relativo consenso acquisito, al momento della consegna della lettera di assunzione; l'informativa aggiornata viene pubblicata sulla intranet aziendale e nella sezione privacy del sito istituzionale di CUP 2000.
- **L'informativa destinata ai fornitori/consulenti** viene inserita, con apposita clausola, nel testo del relativo contratto; il testo esteso dell'informativa viene pubblicato nella sezione privacy del sito istituzionale di CUP 2000.

– **Dati di titolarità dei Soci committenti**

- **L'informativa destinata agli utenti dei servizi gestiti da CUP 2000 S.p.A. per conto dei soci committenti** viene rilasciata solo qualora rientri negli specifici compiti assegnati alla società in qualità di responsabile esterno e di regola al momento dell'accesso ai punti di erogazione ovvero mediante pubblicazione sui portali dedicati.

VIOLAZIONE DEL REGOLAMENTO

Fermi restando i profili di responsabilità civile e penale previsti dalla normativa vigente, con particolare riferimento a condotte di trattamento illecito dei dati (cfr. art. 167 codice privacy) ovvero di omessa adozione di misure minime di sicurezza (cfr. art. 169 codice privacy), in relazione ai dipendenti della Società si precisa che il mancato rispetto del presente Regolamento costituisce un **comportamento sanzionabile disciplinarmente** in quanto grave violazione degli obblighi contrattualmente assunti, con conseguente applicabilità di sanzioni disciplinari (ai sensi del vigente C.C.N.L. e del contratto aziendale).

RINVIO

Per quanto non espressamente disciplinato in questa sede, si rinvia ai principi ed alle disposizioni del Codice Privacy, ai Provvedimenti Generali, le Autorizzazioni Generali ed alle Linee Guida emanate dall'Autorità Garante per la Protezione dei dati personali e, più in generale, alla normativa vigente in tema di protezione di dati personali, che qui deve intendersi integralmente richiamata.

DEFINIZIONI RICHIAMATE DAL CODICE PRIVACY

Ai fini del presente Regolamento, si rinvia all'art. 4 del Codice Privacy. Di seguito si riportano le definizioni di maggiore rilevanza rispetto all'attività aziendale:

"Art. 4. Definizioni:

1. Ai fini del presente codice si intende per:

*a) "**trattamento**", qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;*

*b) "**dato personale**", qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;*

*c) "**dati identificativi**", i dati personali che permettono l'identificazione diretta dell'interessato;*

*d) "**dati sensibili**", i 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;*

*e) "**dati giudiziari**", i 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;*

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

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

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

*i) "**interessato**", la persona fisica cui si riferiscono i dati personali;*

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

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

*n) "**dato anonimo**", il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;*

*o) "**blocco**", la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;*

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

*q) "**Garante**", l'autorità di cui all'articolo 153, istituita dalla legge 31 dicembre 1996, n. 675.*

....OMISSIS....

3. Ai fini del presente codice si intende, altresì, per:

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

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

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

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

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

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

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

*g-bis) "**violazione di dati personali**": violazione della sicurezza che comporta anche accidentalmente la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ai dati personali trasmessi, memorizzati o comunque elaborati nel contesto della fornitura di un servizio di comunicazione accessibile al pubblico."*

....OMISSIS...

1. ORGANIGRAMMA PRIVACY

CUP 2000 S.p.A., in qualità di Titolare del trattamento di dati personali, ha individuato la propria struttura di presidio della privacy.

1.1. TITOLARE DEL TRATTAMENTO

Il Titolare del trattamento ai sensi dell'art. 28 del Codice Privacy è la Società nel suo complesso, che è rappresentata dal Presidente pro-tempore, in qualità di Legale Rappresentante.

1.2. DELEGATO ALLA GESTIONE DELLA PRIVACY

Giusta delibera del Consiglio di Amministrazione del 25 giugno 2014, al Direttore Generale è delegata l'organizzazione interna della tutela della privacy, con la facoltà di nominare uno o più responsabili aziendali nell'ambito delle rispettive competenze, per la raccolta e il trattamento dei dati personali oggetto delle disposizioni di cui al Codice Privacy e/o dei provvedimenti emessi dal Garante per la protezione dei dati personali.

Il Delegato alla gestione della privacy è altresì responsabile esclusivo del riscontro rispetto alle richieste, - da chiunque pervenute anche ai sensi dell'art. 7 del Codice in materia di protezione dei dati personali - di accesso ovvero estrazione di dati di titolarità di CUP 2000 nonché di dati trattati da CUP 2000 in qualità di responsabile esterno del trattamento.

1.3. FUNZIONE AFFARI GENERALI

Il Direttore Generale è supportato dalla Funzione Affari Generali nelle attività delegate di organizzazione e gestione della privacy aziendale. La Funzione coordina la gestione operativa degli adempimenti in materia di privacy, effettua l'istruttoria sulle richieste di accesso o estrazione dati provenienti da soggetti terzi (ad esempio per indagini di polizia giudiziaria ovvero per istanze di accesso ai sensi dell'art. 7 del Codice in materia di protezione dei dati personali); cura gli approfondimenti normativi e verifica, con la collaborazione della Direzione Risorse umane e dei Responsabili di Business Unit e di Funzione, l'applicazione del presente regolamento e di ogni ulteriore disposizione aziendale in materia di privacy, ivi inclusa la corretta preposizione di incaricati ed addetti alla manutenzione nonché l'aggiornamento delle credenziali assegnate a ciascun preposto per l'accesso agli strumenti elettronici di trattamento dei dati effettuate a cura dell'Amministratore di sistema (vedere par. 1.5).

1.4. RESPONSABILI ESTERNI

Ai sensi dell'art. 29 del Codice Privacy, i soggetti esterni che, in qualità di fornitori, consulenti o comunque contraenti, per esigenze organizzative della Società, gestiscono specifici servizi o svolgono attività connesse, strumentali o di supporto a quelle della Società, e che pertanto effettuano attività di trattamento di dati personali di titolarità aziendale (ad es.: fornitura di prestazioni professionali o di prestazioni e servizi anche in convenzione quali consulenti, istituti di credito ed assicurativi,ecc.), sono di norma individuati in qualità di Responsabili del trattamento, sempreché in possesso dei requisiti previsti dall'art. 29 comma 1 del Codice (esperienza, capacità, affidabilità). In alternativa

ovvero nel caso i cui i fornitori/consulenti trattino dati di titolarità dei soci/committenti di CUP 2000 dovrà essere richiesto l'elenco nominativo delle persone fisiche preposte dai fornitori/consulenti alle attività che comportano il trattamento di dati personali e copia delle relative istruzioni operative impartite ai fini delle necessarie verifiche ed integrazioni da parte della società.

1.5. AMMINISTRATORI DI SISTEMA

Il Direttore Generale pro tempore, delegato dal Consiglio di Amministrazione alla gestione ed organizzazione della privacy interna alla società, ha individuato la funzione dell'Amministratore di sistema interno per gli adempimenti in materia di sicurezza informatica previsti dal Codice in materia di protezione dei dati personali e relativo Disciplinare Tecnico (Allegato B del d.Lgs. 196/2003).
Come espressamente stabilito dal Provvedimento del Garante recante "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema del 27 novembre 2008" (G.U. n. 300 del 24 dicembre 2008), successivamente modificato ed integrato, "*l'attribuzione delle funzioni di amministratore di sistema deve avvenire previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza*".

Sulla base di tale valutazione sono stati individuati Amministratori di sistema - con atto di nomina individuale contenente l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato - il Responsabile della Funzione Sviluppo e Tecnologie, i componenti del gruppo di lavoro che eroga servizi sistemistici all'interno della Funzione Sviluppo e Tecnologie ed alcune figure altamente specializzate che svolgono attività analoghe su progetti/servizi.

Gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, sono riportati in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti da parte dell'Autorità Garante.

All'Amministratore di Sistema è assegnata l'attività di gestione tecnica del sistema informatico finalizzata alla sicurezza del trattamento dei dati mediante strumenti elettronici che si concretizza:

- nel garantire la sicurezza dei database in conformità delle prescrizioni del D.Lgs. 196/03 e s.m.i. e del disciplinare tecnico (allegato B) quali, ad esempio:
  - protezione da accesso abusivo;
  - uso e protezione dispositivi di memorizzazione;
  - distruzione e perdita dati;
  - continuità operativa;
- nella predisposizione di idonee e preventive misure di sicurezza informatiche, con particolare riferimento ai seguenti aspetti:
  - Sistema di autenticazione informatica (fornitura gestione e controllo credenziali autenticazione)
  - Sistema di autorizzazione (autorizzazioni per profili di incaricati/addetti e verifica correttezza ambito e persistenza condizioni di conservazione dei profili)

- nella predisposizione di ulteriori misure di sicurezza in caso di trattamento di dati sensibili o giudiziari (verifica rispetto prescrizione del Garante ed adozione procedure per idonea protezione dati sensibili e giudiziari trattati attraverso strumenti elettronici).

Il Responsabile di funzione Sviluppo e Tecnologie, in qualità di Amministratore di Sistema, predispone annualmente per la Direzione Generale apposita relazione in merito alle misure di sicurezza adottate, alle verifiche periodiche sulla corretta assegnazione delle credenziali di incaricati/addetti, al conseguente eventuale aggiornamento dei profili attivi e più in generale sullo stato della sicurezza informatica aziendale.

Amministratore di sistema esterno

Qualora sia necessario individuare un Amministratore di sistema esterno, l'elenco dei nominativi dei soggetti preposti alle specifiche funzioni deve essere comunicato dalle Ditte esterne al Dirigente Responsabile del Servizio e al Referente per la privacy, ai fini della predisposizione della documentazione necessaria alla loro individuazione in qualità di amministratori di sistema.

1.6. INCARICATI DEL TRATTAMENTO

Gli Incaricati del trattamento sono i soggetti - nominati dal Titolare e/o dal Responsabile del trattamento (ex. Art. 29, comma 5 Codice Privacy) - che trattano i dati personali cui hanno accesso attenendosi alle istruzioni loro impartite dal Titolare e/o dal Responsabile.

Le risorse impiegate in mansioni che comportino trattamento di dati personali devono essere appositamente preposte con lettera sottoscritta dal Direttore Generale; i nominativi degli incaricati al trattamento sono forniti alla Funzione Affari Generali dalle Business Unit e dalle Funzioni, in accordo con la Direzione risorse umane, unitamente all'indicazione della Unità di trattamento/di manutenzione di riferimento.

1.7. ADDETTI ALLA MANUTENZIONE E GESTIONE

L'allegato B al Codice Privacy, recante "Disciplinare tecnico in materia di misure minime di sicurezza" prevede espressamente anche la figura degli "addetti alla gestione o alla manutenzione degli strumenti elettronici".

CUP 2000 ha individuato espressamente alcune "unità di manutenzione" che comprendono le attività di gestione e manutenzione delle banche dati. Per questa particolare tipologia di addetti sono redatte ulteriori e specifiche istruzioni operative (cfr. par. 4)

1.8. UNITÀ DI TRATTAMENTO

CUP 2000 ha individuato le Unità di trattamento/di manutenzione, ai sensi dell'art. 30, comma 2 del Codice in materia di protezione dei dati personali, indicando per ciascuna le banche dati di riferimento e le singole operazioni di trattamento sui dati personali/sensibili/giudiziari che ciascun preposto è autorizzato a compiere.

Tale mappatura è preliminare alla verifica sulla correttezza dell'attuale assegnazione delle credenziali rispetto all'effettiva preposizione alle attività nonché all'aggiornamento delle lettere di nomina e delle relative istruzioni operative.

Il documento è allegato al presente Regolamento e ne costituisce parte integrante e sostanziale. (all. 1)

2. REGOLE OPERATIVE

REGOLE GENERALI PER TUTTI I TRATTAMENTI

Come stabilito all'art. 11 del Codice Privacy, i dati personali oggetto del trattamento devono essere:

- **trattati in modo lecito e secondo correttezza**;
- **raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi**;
- **esatti e, se necessario, aggiornati**;
- **pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati**;
- **conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati**.

Inoltre:

- i dati personali trattati in violazione della normativa in materia di protezione dati personali dei dati **NON POSSONO ESSERE UTILIZZATI** (art. 11 co.2 Codice Privacy)

- i dati idonei a rivelare lo stato di salute **NON POSSONO ESSERE DIFFUSI** (art. 22 co 8, Codice Privacy)

Si rende necessario individuare regole operative comuni a tutti coloro che trattano a vario titolo dati personali nell'esercizio delle mansioni lavorative aziendali, dettagliando successivamente ulteriori modalità operative particolari a seconda della tipologia di dati trattati (personali, sensibili/giudiziari) piuttosto che in base agli strumenti che vengono utilizzati per il trattamento.

Le seguenti prescrizioni sono da intendersi VINCOLANTI per i dipendenti della Società che siano preposti in qualità di incaricati del trattamento/addetti alla manutenzione e gestione.
SANZIONI ED ISPEZIONI: l'eventuale violazione delle disposizioni di seguito riportate ~~o~~ costituisce un illecito, che può comportare l'applicazione di sanzioni di natura disciplinare ma anche di natura civile e penale, secondo quanto previsto dal codice della privacy. Si ricorda, inoltre, che è stato siglato un protocollo d'intesa tra la Guardia di Finanza e l'Autorità Garante per la protezione dei dati personali per una sempre più intesa ed efficace attività di controllo sulla raccolta dei dati. Si auspica una responsabile e consapevole collaborazione da parte di tutti gli incaricati nella diligente osservanza delle disposizioni di legge e nelle prescrizioni contemplate all'interno del presente modello ai fini di un corretto trattamento dei dati personali e tutela della privacy.

1. Ciascun preposto è tenuto a rispettare i **principi generali previsti dal Codice Privacy**, con particolare riferimento alla liceità e correttezza del proprio agire: il preposto può lecitamente effettuare le operazioni di trattamento secondo **le modalità e le finalità espressamente stabilite per ciascuna Unità di**

trattamento/manutenzione di appartenenza, giusta espressa preposizione per iscritto.

2. Il trattamento di dati personali deve essere effettuato in misura pertinente e non eccedente, esclusivamente per **le finalità per le quali i dati sono stati raccolti e nella misura in cui queste sono state oggetto di apposita informativa** fornita agli interessati, come previsto dall'art. 13 del Codice Privacy;

3. Il trattamento di dati personali **non deve essere effettuato** qualora sia possibile realizzare le finalità per cui è attuato **attraverso l'uso di dati anonimi**;

4. Le attività di trattamento dei dati personali e sensibili devono essere **limitate al tempo strettamente necessario al raggiungimento degli scopi** per cui i dati medesimi sono stati raccolti o sono successivamente trattati;

5. A seguito della preposizione alla relativa Unità di trattamento/manutenzione, ed in relazione alle operazioni consentite secondo il profilo di attività assegnato, ciascun incaricato/addetto alla manutenzione è dotato di **credenziali di autenticazione** (user id + password ovvero dispositivi smart card) riservate e personali che consentono di accedere ai dati personali che è autorizzato a trattare, nonché ad utilizzare gli strumenti aziendali necessari per il trattamento. (cfr. par. 5.a). Le credenziali vengono disattivate al momento della cessazione del rapporto di lavoro, previa comunicazione all'Amministratore di Sistema da parte della Direzione Risorse Umane, ovvero aggiornate, su richiesta dei responsabili, in caso di preposizione ad altra unità di trattamento o di modifica dell'ambito di trattamento consentito.

6. Ciascun soggetto preposto allo svolgimento delle operazioni di trattamento ha **l'obbligo di mantenere il segreto sui dati raccolti o di cui venga a conoscenza** nel corso della propria attività lavorativa, evitando di diffonderli o di comunicarli a terzi o comunque a soggetti non legittimati al trattamento di tali informazioni. Non è pertanto autorizzato a fornire riscontro diretto a richieste, verbali o scritte, di estrazione o di comunicazione di dati di titolarità della società ovvero di titolarità di terzi, anche qualora tali richieste pervengano da uffici o strutture aziendali se non autorizzate all'accesso ai dati medesimi. Di tali richieste dovrà essere data apposita informativa alla Direzione Generale ai fini delle necessarie verifiche e dell'eventuale formalizzazione del riscontro.

7. In caso di allontanamento dal proprio ufficio o dalla propria postazione di lavoro, ciascun soggetto preposto allo svolgimento delle operazioni di trattamento deve adottare tutte l**e accortezze e precauzioni al fine di impedire l'accesso fisico** a chi non sia legittimato, soprattutto se esterno all'organizzazione di appartenenza o non specificamente autorizzato;

8. Qualora l'incaricato utilizzi, nello svolgimento delle proprie mansioni, atti/documenti contenenti dati personali o sensibili, questi **non devono essere lasciati incustoditi** ma occorre siano evitati eventuali accessi o la conoscenza da parte di soggetti non autorizzati; alla fine del ciclo di lavoro, la documentazione deve essere SEMPRE riposta negli archivi ad accesso controllato;

9. Al momento della registrazione dei dati raccolti, occorre **prestare attenzione alla digitazione e all'inserimento dei dati identificativi e degli altri dati riferiti**

all'interessato, al fine di evitare errori, che potrebbero generare problemi nella corretta gestione delle anagrafiche e nello svolgimento delle operazioni, che caratterizzano il processo di trattamento;

10. I preposti alla **duplicazione di documentazione** (con stampanti o fotocopiatrici o altre periferiche) ovvero che utilizzando strumenti per la riproduzione cartacea di documenti digitali, **sono tenuti a procedere alla relativa distruzione del supporto**, qualora si verifichino errori o la riproduzione non sia corretta, evitando di riutilizzare i fogli.

3. MISURE DI SICUREZZA

L'art. 31 del Codice Privacy stabilisce che i dati personali oggetto del trattamento devono essere "*custoditi e controllati anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati ed alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita anche accidentale dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta*."
L'omessa adozione delle misure minime, di cui al "Disciplinare tecnico in materia di misure minime di sicurezza" (Allegato B al Codice in materia di protezione dei dati personali) è rilevante ai sensi dell'art. 169, comma 1 del Codice.
Le misure minime di sicurezza obbligatorie si differenziano a seconda della modalità del trattamento dei dati e pertanto sono di seguito individuate :

- ***MISURE MINIME PER TRATTAMENTI EFFETTUATI CON STRUMENTI ELETTRONICI***

Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati/addetti dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa ad uno specifico trattamento o ad un insieme di trattamenti.

Gestione delle credenziali di autenticazione
Gli incaricati del trattamento e gli addetti alla manutenzione e gestione devono utilizzare e gestire le proprie credenziali di autenticazione (composte dal Codice identificativo c.d. USER-ID associato ad una password riservata, un dispositivo di autenticazione - es. smart card- ovvero una caratteristica biometrica) attenendosi alle seguenti istruzioni:

- Le user-id individuali per l'accesso alle applicazioni NON devono essere mai condivise tra più utenti, anche se preposti alla medesima unità di trattamento; nel caso in cui altri utenti debbano accedere ai medesimi dati è necessaria una espressa autorizzazione scritta;
- La user-id già assegnata NON può essere attribuita ad alcun altro incaricato, anche se in tempi differenti
- Gli strumenti di autenticazione (password, dispositivi smart card ecc..) devono essere mantenuti riservate e NON devono mai essere condivisi con altri utenti, anche se preposti alla medesima unità di trattamento.
- Le credenziali di autenticazione non utilizzate da almeno 6 mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica;
- Le credenziali di autenticazione sono disattivate a seguito della perdita della qualità che consente all'incaricato/addetto l'accesso ai dati personali;
- Ulteriori indicazioni per la corretta gestione delle password:
  - Impostare la password con una lunghezza di almeno 8 caratteri o comunque pari al massimo consentito dal sistema;
  - Individuare una password che non contenga riferimenti facilmente riconducibili all'incaricato;
  - Mantenere la password riservata e non divulgarla a terzi
  - Non trascrivere la password su fogli, agendine, post-it facilmente accessibili a terzi;
  - La password eventualmente assegnata per il primo accesso è modificata dall'incaricato al primo utilizzo e successivamente deve essere sostituita ogni 3 mesi (in caso consenta l'accesso a dati sensibili) e comunque secondo le indicazioni ricevute;

  - Non includere la password in processi di connessione automatica;
  - Qualora una password perda di segretezza, l'incaricato provvedere immediatamente alla sua sostituzione
- Gli eventuali dispositivi di autenticazione forniti in possesso ed uso esclusivo dell'incaricato devono essere custoditi con cura e diligenza;
- Nel caso in cui la sessione di lavoro sia interrotta, l'incaricato non deve lasciare incustodito lo strumento di trattamento né consentirne l'accesso ad altri, provvedendo a mettere "in sicurezza" la macchina da cui ha effettuato l'accesso ai dati personali.

Gestione degli strumenti elettronici in dotazione

Ciascun incaricato è responsabile del corretto utilizzo e della custodia degli strumenti elettronici in dotazione (a titolo esemplificativo personal computer, periferiche, lettori di smart card,…). Devono essere adottate le misure di sicurezza per la tutela della riservatezza, consistenti nell'evitare che l'accesso ai dati possa avvenire da parte di soggetti estranei all'organizzazione o non specificamente autorizzati.
Per monitorare il rispetto delle politiche e degli obblighi di sicurezza possono essere svolti controlli a campione mediante la raccolta e l'analisi di dati aggregati e anonimi.
Nel caso di provato o constatato uso illecito o non consentito degli strumenti elettronici, risultante dalla verifica delle informazioni in modalità aggregata e anonima, può essere necessario procedere alla verifica delle registrazioni delle sessioni di lavoro, al fine di sanzionare condotte illecite, anche su richiesta dell'autorità giudiziaria, cui le informazioni potranno essere comunicate, senza alcuna specifica informativa all'interessato.

Gestione della posta elettronica

L'uso della posta elettronica è autorizzato esclusivamente per finalità di lavoro; è raccomandato di non inviare comunicazioni a soggetti estranei agli scopi istituzionali o professionali. In caso di assenza prolungata può essere richiesto all'incaricato di individuare un proprio fiduciario autorizzato ad accedere alla casella assegnata dal titolare o dal responsabile del trattamento. Nell'ipotesi in cui la email debba essere utilizzata per la trasmissione di dati sensibili, si raccomanda di prestare attenzione a che:

- l'indirizzo del destinatario sia stato correttamente digitato;
- l'oggetto del messaggio non contenga direttamente il riferimento a stati, fatti o qualità idonei a rivelare dati di natura sensibile;
- nel corpo del messaggio sia presente un'intestazione standardizzata in cui si avverta della confidenzialità/riservatezza del messaggio.

Salvataggio di dati

Qualora non sia previsto un sistema di salvataggio di dati personali automatico ovvero centralizzato, con cadenza almeno settimanale devono essere effettuate copie di sicurezza dei dati personali oggetto di trattamento, utilizzando gli apparati eventualmente messi a disposizione da parte di CUP 2000.

Antivirus e protezione dei dati

Qualora non siano attivi sistemi automatici di aggiornamento dei sistemi di protezione da programmi antivirus, gli incaricati devono procedere all'effettuazione delle operazioni di aggiornamento, di volta in volta richieste dal sistema, secondo le istruzioni visualizzate sullo schermo; tutti i supporti di memorizzazione devono essere sottoposti a scansione antivirus.

Gestione organizzativa e tecnica dei supporti di memorizzazione dei dati

Nel caso si utilizzino supporti informatici per il trattamento di dati personali, sono previste ulteriori misure di sicurezza:

- i supporti informatici che contengono dati sensibili o giudiziari sono distrutti/resi inutilizzabili ovvero possono essere riutilizzati solo dopo avere provveduto a cancellare i dati e le informazioni contenute in modo tale che questi non siano tecnicamente in alcun modo recuperabili;

- ***MISURE MINIME PER TRATTAMENTO DI DATI EFFETTUATI CON ATTI E DOCUMENTI CARTACEI O STRUMENTI NON ELETTRONICI***

  Nel caso in cui il trattamento sia effettuato con strumenti diversi da quelli elettronici, gli incaricati devono:

  - verificare che siano rispettati i criteri di controllo e custodia per tutto il ciclo di lavorazione necessario allo svolgimento delle operazioni di trattamento effettuate tramite atti e/o documenti; in particolare qualora i documenti contenenti i dati personali siano affidati direttamente all'incaricato, questo è tenuto a controllarli e custodirli in modo da impedire l'accesso a persone non autorizzate fino alla restituzione all'esito delle operazioni di trattamento effettuate.
  - L'accesso agli archivi contenenti dati sensibili e giudiziari deve essere controllato; chi vi accede dopo l'orario di lavoro a qualsiasi titolo deve essere identificato e registrato e qualora gli archivi siano sprovvisti di strumenti elettronici per il controllo degli accessi le persone che vi hanno accesso sono preventivamente autorizzate;
  - Nel caso in cui sia necessario effettuare trasmissioni o riproduzione di documenti contenenti dati personali devono essere adottate le successive cautele:
    - NON lasciare incustoditi presso fax, stampanti e fotocopiatrici documenti contenenti dati personali;
    - In caso di trasmissione via fax di documenti contenenti dati personali verificare, eventualmente per via telefonica, l'avvenuta ricezione del fax e, una volta trasmessi ritirarli immediatamente.

4. ISTRUZIONI SPECIFICHE PER PREPOSTI ED AMMINISTRATORE DI SISTEMA

In attuazione al presente regolamento sono redatte le seguenti istruzioni operative che costituiscono parte integrante delle lettere di nomina degli Incaricati del trattamento, degli Amministratori di Sistema e degli Addetti alla manutenzione:

INCARICATI DEL TRATTAMENTO

Le presenti istruzioni sono impartite ai sensi dell'art. 30 del d. lgs. 196/2003 (codice della privacy) e devono essere osservate da ciascuna persona fisica autorizzata ad accedere ai dati personali e preposta allo svolgimento delle operazioni di trattamento relativa a dati di titolarità di CUP 2000 ovvero rispetto ai quali la società è stata nominata responsabile esterno dai soci committenti.
Si ricorda che:

costituisce "**trattamento**" qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati

In particolare, ciascun incaricato del trattamento deve:

- rispettare i principi generali previsti dall'art. 11 (modalità del trattamento e requisiti dei dati) del codice privacy, con particolare riferimento alla liceità e correttezza del proprio agire, all'obbligo di procedere alla raccolta e alla registrazione dei dati per scopi determinati, espliciti e legittimi, comunque connessi alla mission e all'ambito di operatività assegnato. Si ricorda, altresì, che i dati devono trattati nei limiti della pertinenza, completezza e non eccedenza rispetto alle finalità per cui sono raccolti o successivamente trattati;
- **rispettare l'obbligo di riservatezza e segretezza** e conseguentemente il divieto di comunicazione e diffusione dei dati trattati nel corso dell'incarico svolto;
- utilizzare i dati, cui abbia accesso, solamente per finalità compatibili all'esecuzione delle proprie mansioni o dei compiti affidati, per cui è autorizzato ad accedere alle informazioni e ad utilizzare gli strumenti aziendali.

L'incaricato, inoltre, deve:

- rispettare le misure di sicurezza minime (indicate nell'allegato B al codice privacy) e le misure idonee adottate dalla società, atte a salvaguardare la riservatezza e l'integrità dei dati, ai sensi degli articoli 31 e seguenti del codice privacy;
- segnalare eventuali malfunzionamenti di strumenti elettronici, perdite di dati o esigenze (sia di natura organizzativa, sia tecnica), che possano migliorare lo svolgimento delle operazioni affidate;

- accedere ai dati strettamente necessari all'esercizio delle proprie funzioni e competenze, ai sensi dell'art. 30 del Codice del codice della privacy.

MODALITÀ DI SVOLGIMENTO DELLE OPERAZIONI: (MODALITÀ SPECIFICHE CHE RIGUARDANO SOLO ALCUNI INCARICATI)

- **identificazione dell'interessato**: al momento della raccolta dei dati personali, qualora sia necessario individuare l'identità del soggetto che fornisce le informazioni, è obbligatorio richiedere un documento di identità o di riconoscimento, al fine di verificare la identità e di procedere correttamente alla raccolta e alla registrazione delle informazioni;
- **verifica del controllo dell'esattezza del dato e della corretta digitazione**: al momento della registrazione dei dati raccolti, occorre prestare attenzione alla digitazione e all'inserimento dei dati identificativi e degli altri dati riferiti all'interessato, al fine di evitare errori, che potrebbero generare problemi nella corretta gestione dell'anagrafica e nello svolgimento delle operazioni, che caratterizzano il processo di trattamento;
- **accesso fisico ai locali**: i locali, ove sono custoditi i dati personali (ed in particolare quelli di natura sensibile), devono essere soggetti a controllo e a verifica, al fine di evitare che durante l'orario di lavoro possano essere conosciuti o accessibili da parte di soggetti non autorizzati. Si raccomanda, in caso di allontanamento dal proprio ufficio o dalla propria postazione di lavoro, di adottare tutte le accortezze e precauzioni al fine di impedire l'accesso fisico a chi non sia legittimato, soprattutto se esterno all'organizzazione di appartenenza.

ISTRUZIONI PER L'USO DEGLI STRUMENTI DEL TRATTAMENTO

a) **strumenti elettronici**: ciascun incaricato è responsabile del corretto utilizzo e della custodia degli strumenti elettronici in dotazione (a titolo esemplificativo personal computer, periferiche, lettori di smart card,…). Si devono adottare le misure di sicurezza per la tutela della riservatezza, consistenti nell'evitare che l'accesso ai dati possa avvenire da parte di soggetti estranei all'organizzazione o non specificamente autorizzati. Al fine di verificare il corretto utilizzo degli strumenti in dotazione potranno essere svolti controlli a campione mediante la raccolta e l'analisi di dati aggregati e anonimi. Inoltre, nel caso di provato o constatato uso illecito o non consentito degli strumenti elettronici, risultante dalla verifica delle informazioni in modalità aggregata e anonima, può essere necessario procedere alla verifica delle registrazioni delle sessioni di lavoro, al fine di sanzionare condotte illecite, anche su richiesta dell'autorità giudiziaria, cui le informazioni potranno essere comunicate, senza alcuna ulteriore informativa all'interessato;
b) **posta elettronica**: l'uso della posta elettronica è autorizzato esclusivamente per finalità di lavoro, per cui si raccomanda di non inviare comunicazioni a soggetti estranei agli scopi istituzionali o professionali. Si informa che in caso di assenza prolungata può essere richiesto all'incaricato di individuare un proprio fiduciario autorizzato ad accedere alla casella assegnata dal titolare o dal responsabile del trattamento. Nell'ipotesi in cui la email debba essere utilizzata per la trasmissione di dati sensibili, si raccomanda di prestare attenzione a che:
    - l'indirizzo del destinatario sia stato correttamente digitato,
    - l'oggetto del messaggio non contenga direttamente il riferimento a stati, fatti o qualità idonei a rivelare dati di natura sensibile;

- nel corpo del messaggio sia presente un'intestazione standardizzata in cui si avverta della confidenzialità/riservatezza del messaggio;

c) **distruzione delle copie cartacee**: coloro che sono preposti alla duplicazione di documentazione (con stampanti o fotocopiatrici o altre periferiche) ovvero che utilizzando strumenti per la riproduzione cartacea di documenti digitali, sono tenuti a procedere alla relativa distruzione del supporto, qualora si verifichino errori o la riproduzione non sia corretta, evitando di riutilizzare i fogli, salva l'ipotesi di uso esclusivamente personale per eventuali appunti o brutte copie, da distruggere immediatamente quando non più necessarie;

d) **atti e documenti cartacei**: gli atti e i documenti, contenenti dati personali o sensibili, non devono essere lasciati incustoditi, ma occorre che gli incaricati, cui essi sono affidati per lo svolgimento delle loro mansioni, controllino eventuali accessi o la conoscenza da parte di soggetti non autorizzati. Alla fine del ciclo di lavoro, la documentazione deve essere riposta negli archivi ad accesso controllato.

ISTRUZIONI IN TEMA DI SICUREZZA

a) accessi a strumenti elettronici mediante utilizzo di credenziali di autenticazione:
   - accesso ai sistemi di CUP 2000: la parola chiave, assegnata a ciascun incaricato da parte di CUP2000 è composta da un numero di caratteri almeno pari a otto o comunque pari al numero massimo di caratteri consentito dal sistema. Ciascun incaricato, nel gestire la propria password deve:
     - provvedere alla sostituzione immediata della password assegnata, secondo le modalità operative previste dal sistema, e successivamente cambiare la propria credenziale con cadenza almeno trimestrale;
     - nel procedere alla sostituzione e al cambio periodico, ciascun incaricato deve adottare una password di lunghezza almeno pari a quella che gli è stata precedentemente assegnata;
     - scegliere una password che non deve contenere riferimenti agevolmente riconducibili alla sfera personale o all'identità all'incaricato medesimo;
     - evitare di divulgare o comunicare a terzi la password che deve essere segreta e non lasciata incustodita, con avvertimento che ogni accesso a strumenti elettronici mediante utilizzo della componente riservata della credenziale assegnata è imputabile al soggetto che ne risulta titolare, con conseguente onere e obbligo di provare l'uso indebito e non autorizzato;

b) **back-up:** salvo che non sia previsto un sistema di salvataggio di dati personali automatico ovvero centralizzato, occorre procedere con cadenza almeno settimanale alla effettuazione di copie di sicurezza dei dati personali oggetto di trattamento, per le finalità di cui in premessa, utilizzando gli apparati eventualmente messi a disposizione da parte di CUP 2000;

c) **antivirus:** a meno che non siano adottati sistemi automatici di aggiornamento dei sistemi di protezione da programmi antivirus, gli incaricati devono procedere all'effettuazione delle operazioni di aggiornamento, di volta in volta richieste dal sistema, secondo le istruzioni visualizzate sullo schermo

d) **protezione degli strumenti di lavoro:** in caso di assenza, anche momentanea, dalla propria postazione di lavoro, adottare misure atte a escludere che soggetti non autorizzati possano acquisire informazioni o accedere alle banche dati gestite. A tal proposito, a titolo meramente esemplificativo, si consiglia di adottare un sistema di oscuramento (cd. ***screen-saver***) dotato di password, ovvero uscire dal

programma che si sta utilizzando, ove sia protetto da parola chiave, ovvero, in alternativa, spegnere l'elaboratore che si sta utilizzando.

AMMINISTRATORI DI SISTEMA

Compiti ed attribuzioni dell'Amministratore di sistema (con attività differenziate a seconda del profilo proprio dell'Amministratore di sistema e dei compiti attribuiti dal Responsabile della Funzione):

a) **gestire le credenziali di autenticazione** dei responsabili e dei soggetti incaricati del trattamento/addetti alla manutenzione;
b) **gestire i profili di autorizzazione** degli incaricati al trattamento dei dati/addetti alla manutenzione, su specifiche indicazioni impartite dai responsabili del trattamento;
c) **provvedere alla disattivazione/variazione** delle utenze assegnate al personale cessato dal servizio o che abbia modificato il proprio ambito di trattamento, su richiesta specifica dei responsabili;
d) **pianificare la formazione del personale** dell'Area Sistemi Informativi, in materia di soluzioni tecniche per la garanzia della sicurezza dei dati e della protezione degli strumenti elettronici;
e) **custodire la documentazione cartacea**, prodotta nello svolgimento dei propri compiti istituzionali.

Compiti da gestire direttamente ovvero anche tramite addetti alla manutenzione e gestione degli strumenti elettronici:

a) adottare i provvedimenti necessari ad **evitare la perdita o la distruzione dei dati** e provvedere al loro ricovero periodico con **copie di back-up** secondo i criteri stabiliti;
b) **assicurarsi della qualità delle copie di back-up** dei dati e della loro conservazione in luogo adatto e sicuro;
c) **prevedere procedure operative per la disattivazione dei "codici identificativi personali" (User-ID)**, in caso di perdita della qualità di incaricato all'accesso all'elaboratore, oppure nel caso di **mancato utilizzo** dei "codici identificativi personali" (User-ID) per un **periodo superiore a 3 mesi**;
d) **proteggere gli strumenti elettronici dal rischio di intrusione** (violazione del sistema da parte di "hackers") e dal rischio di programmi virus mediante idonee misure di sicurezza da aggiornare **almeno ogni 6 mesi**;
e) mantenere un **adeguato sistema di autorizzazione** che, per ogni identificativo utente, riporti la **data di attivazione**, **le funzioni del sistema** alle quali l'utente è abilitato, **la data di cessazione dell'identificativo** stesso;
f) **provvedere al salvataggio dei dati** presenti sui server e al loro **ripristino** in caso di necessità;
g) **conservare le copie di back-up**;
h) **registrare e archiviare tutte le attività eseguite sul sistema**;
i) **garantire** che **le informazioni scambiate** con soggetti interni ed esterni siano opportunamente **protette da rischi di intrusione**.

Funzioni di controllo e vigilanza nei confronti di <u>fornitori di strumenti elettronici e di addetti esterni alla gestione e manutenzione di strumenti elettronici:</u>

a) **l'hardware sia conforme alla normativa** in materia di protezione dei dati personali, con particolare riferimento al rispetto del principio di necessità, di cui all'art. 3 del codice privacy;

b) in occasione di ciascun intervento di manutenzione e di assistenza tecnica, sottoscrivano un **verbale sulla esecuzione dei lavori**, che attesti la conformità alle regole dette;
c) i **software operativi e i programmi applicativi siano idonei ad assicurare**:
   - la **separazione tra dati anagrafici e dati sensibili**, ovvero la **cifratura** dei dati idonei a rivelare lo stato di salute, ai sensi dell'art. 22, comma 6 e del punto 24 dell'allegato B del codice privacy;
   - la **tracciabilità delle attività degli utenti**, nel rispetto del codice privacy e delle garanzie di tutela dei dipendenti;
   - un **sistema di autenticazione e di autorizzazione conforme** alla normativa in materia di protezione dei dati personali;

d) i **fornitori di piattaforme di data base debbono garantire la tracciabilità** delle transazioni degli utenti.

Funzioni di controllo e di vigilanza da porre in essere al fine di una corretta gestione della privacy aziendale (Responsabile di funzione):

a) **verificare l'adozione delle misure minime di sicurezza**;
b) **verificare lo stato di adozione delle misure idonee di sicurezza**;
c) **pianificare regolari controlli della vulnerabilità** dei programmi per elaboratore;
d) **verificare gli eventi** che hanno causato **rischi** per l'integrità e la disponibilità dei dati personali;
e) pianificare attività di **audit interno**, finalizzata al controllo del rispetto delle istruzioni operative e delle misure di sicurezza;
f) **verificare il rispetto delle istruzioni** impartite ai responsabili e agli incaricati del trattamento/addetti alla manutenzione;
g) **verificare la congruità delle misure di sicurezza organizzative**, **fisiche** e **logiche** ad oggi esistenti, e perseguire l'obiettivo di raggiungere un livello di protezione idoneo con particolare riferimento alle recenti disposizioni in materia di trattamento e protezione di dati personali ai sensi del D.Lgs. 196/2003;
h) **comunicare** a tutti gli incaricati del trattamento/addetti alla manutenzione le **misure da predisporre e/o rispettare** per la protezione dei dati di loro competenza, ponendo in essere tutte quelle forme di controllo nel tempo che si riterranno opportune previa comunicazione per approvazione al Titolare.
i) **monitorare lo stato delle misure di sicurezza** utilizzando apposita check-list;
j) redigere **apposita relazione scritta** sulla gestione delle attività assegnate, con particolare riferimento alle misure di sicurezza adottate, alle verifiche periodiche sulla corretta assegnazione delle credenziali di incaricati/addetti, al conseguente eventuale aggiornamento dei profili attivi e più in generale sullo stato della sicurezza informatica aziendale.

ADDETTI ALLA MANUTENZIONE

Le seguenti istruzioni devono essere osservate dai preposti in qualità di addetti alla gestione o manutenzione che trattano dati di titolarità di CUP 2000/per i quali CUP 2000 è nominata responsabile esterno del trattamento nonché dagli addetti di ditte specializzate che svolgano interventi tecnici di gestione e manutenzione degli strumenti elettronici su richiesta di CUP 2000:

- Effettuare **operazioni di manutenzione e supporto** per verifica corretto funzionamento (monitoraggio e diagnostica) su flussi dei dati;
- **gestire le credenziali di autenticazione** dei soggetti incaricati del trattamento su indicazione dell'Amministratore di sistema;
- **gestire i profili di autorizzazione** degli incaricati al trattamento dei dati, su specifiche impartite dai responsabili di funzione/BU, su indicazione dell'Amministratore di sistema;
- provvedere alla **disattivazione/variazione delle utenze**, ivi compreso l'account di posta elettronica, assegnate al personale cessato dal servizio o che abbia modificato il proprio ambito di trattamento, su richiesta specifica dei responsabili ovvero della Direzione Risorse Umane e su indicazione dell'Amministratore di sistema;
- **custodire la documentazione cartacea**, prodotta nello svolgimento dei propri compiti istituzionali;

L'accesso agli addetti alla gestione e manutenzione è consentito unicamente ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere alle operazioni di manutenzione dei programmi o del sistema informatico.
A ciascun addetto alla manutenzione, previa sottoscrizione di apposito atto per accettazione, è pertanto consentito eseguire le operazioni strettamente necessarie a tali scopi e/o richieste dal titolare, secondo le seguenti istruzioni operative:

- Nel caso in cui sia necessario effettuare stampe di prova per controllare il funzionamento di stampanti o per verificare il funzionamento di strumenti o programmi installati, non utilizzare files già esistenti ma creare files di prova.
- Nel caso si renda strettamente necessario accedere a files contenenti dati (ad esempio per il recupero di un testo) limitare l'accesso ai dati per il tempo strettamente necessario all'assolvimento delle operazioni di manutenzione.
- Per effettuare operazioni di manutenzione sui database aziendali che prevedano la raccolta e la conservazione dei dati, tali dati dovranno essere custoditi in modo tale da non essere accessibili da soggetti non autorizzati.
- Devono inoltre essere adottate le misure di sicurezza minime previste dal codice in materia di protezione dei dati personali;
- E' necessario informare al più presto il titolare o il responsabile del trattamento qualora si dovessero riscontrare malfunzionamenti o non conformità.
- Tutti i dati personali contenuti nei data base devono essere protetti da password;
- Nel caso in cui sia necessario accedere ai dati attraverso gli strumenti elettronici in dotazione agli incaricati, attenersi alle seguenti indicazioni:
    - in presenza dell'incaricato, far digitare la password dall'incaricato stesso evitando di venirne a conoscenza;

  - in assenza dell'incaricato rivolgersi alla persona individuata dall'incaricato quale proprio fiduciario il quale provvederà all'inserimento della password.
- Nei casi in cui sia necessario accedere ai dati personali attraverso il server, rivolgersi all'amministratore di sistema o provvedere, in collaborazione con l'amministratore di sistema stesso, alla creazione di credenziali di autenticazione da utilizzarsi esclusivamente per l'accesso da parte degli addetti alla manutenzione/gestione dei sistemi informatici;
- L'amministratore di sistema ha facoltà, in qualunque momento di controllare e verificare l'operato degli addetti alla manutenzione;
- Qualora si renda necessario prelevare apparecchiature elettroniche per effettuare attività di ripristino o interventi di manutenzione che comportino il reset di password precedentemente individuate, la nuova password di accesso sarà comunicata all'incaricato il quale provvederà a cambiarla al termine delle operazioni di manutenzione;
- l'accesso al sistema informatico da parte degli addetti alla manutenzione/gestione del sistema è consentito unicamente previo inserimento di password e ID;
- E' assolutamente vietato comunicare o diffondere i dati personali di qualsiasi natura provenienti dai database gestiti dalla società, se non previa espressa comunicazione scritta;
- Nel caso in cui CUP 2000 si avvalga di soggetti esterni per interventi specialistici che comportino trattamento di dati personali deve essere rilasciata una dichiarazione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni in materia di misure minime di sicurezza.