Privacy Policy di CUP 2000 S.c.p.A.

Approvata con Determina dell'Amministratore Unico n. 25 del 22 Novembre 2018

CUP 2000 S.c.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

1. Adempimenti in materia di dati personali

1.1. Premessa

La Società CUP 2000 S.c.p.A. è da sempre particolarmente sensibile alla riservatezza ed alla sicurezza dei dati personali, propri e di terze parti. Per tale motivo ha uniformato il proprio modo di trattare i dati personali ai dettati del *Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati*) (di seguito GDPR o Regolamento Privacy), prevedendo, altresì, misure di sicurezza adeguate a quanto richiesto dalla norma.

La riservatezza delle persone fisiche attraverso la corretta acquisizione, gestione e circolazione dei dati personali e mediante l'adozione di idonee misure di sicurezza per la loro protezione è tutelata dal citato Regolamento, nonché, in quanto non incompatibili, dalle singole normative nazionali e dai provvedimenti dell'Autorità Garante per la Protezione dei Dati Personali.

Il Regolamento afferma importanti principi quali il diritto alla protezione dei dati personali e quello della necessità del trattamento (*need to know*) e, al contempo, garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale, al diritto alla protezione dei dati personali, alla portabilità dei dati, sino al diritto all'oblio.

I principi fondamentali introdotti dal Regolamento e non presenti nel precedente "Codice Privacy" (dec. legisl. 196/03), possono essere riassunti come segue:

- Privacy by design e by default;
- Rafforzamento del principio del "need to know";
- Introduzione di adempimenti formali come l'adozione del Registro dei Trattamenti e redazione del PIA – Privacy Impact Assessment;
- Nuovi diritti degli interessati;
- Obbligo di gestione dei Data Breaches;
- Determinazione delle misure di sicurezza secondo un approccio "risk based";
- Introduzione della figura del DPO – Data Protection Officer (Responsabile della Protezione dei Dati Personali);
- Ridefinizione della figura del Responsabile del Trattamento dei Dati Personali e del Contitolare del trattamento;
- Forte inasprimento delle sanzioni che, in caso di inadempimento, possono arrivare sino a € 20 milioni o al 4% del fatturato annuo worldwide.

Il Regolamento specifica, altresì, che il trattamento dei dati è disciplinato assicurando un elevato livello di tutela dei diritti e delle libertà nel rispetto dei principi di semplificazione,

armonizzazione ed efficacia delle modalità previste per il suo esercizio da parte degli interessati, nonché per l'adempimento degli obblighi da parte dei titolari del trattamento.

Il Regolamento si compone di 173 "considerande" e di 99 articoli.

Il presente documento contiene la Politica definita da CUP 2000 (nel seguito la "Società") per adempiere alle prescrizioni del Regolamento. Esso contiene le indicazioni per l'effettuazione degli adempimenti necessari verso l'Autorità Garante (quali la notificazione dei trattamenti e dei Data Breaches), verso i soggetti interessati (quali l'informativa, la raccolta del consenso al trattamento, laddove necessario, il riscontro delle richieste di esercizio del diritto d'accesso) e verso le strutture operative (quali le nomine e le istruzioni agli Autorizzati ed agli eventuali Responsabili del trattamento ed al Responsabile per la Protezione dei Dati Personali).

1.2. Ambito oggettivo

Il Regolamento si applica alle attività che comportano il trattamento dei dati personali di titolarità di CUP 2000 S.c.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 la società sia stata individuata, ai sensi dell'art. 28 del Regolamento Privacy, in qualità di responsabile 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 della società in qualità di responsabile 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 Regolamento UE ed ai consensi acquisiti dagli interessati, o ex art. 14 del medesimo Regolamento se i dati non siano stati ottenuto presso l'interessato.

1.3. Definizioni

Preliminarmente, al fine di una corretta interpretazione degli adempimenti che saranno menzionati nel seguito, si fornisce un'esplicitazione dei termini utilizzati nel Regolamento.

In particolare si intende per:

1) «dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere individuata, direttamente o indirettamente, con particolare riferimento a un dato come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

2) «trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

3) «limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

4) Privacy by Design e Privacy by Default: l'art. 25 del GDPR prevede in capo al Titolare del Trattamento due modalità di gestione del Modello Privacy interno della propria azienda. La prima, prevista al comma 1 dell'art. 25 è definita privacy by Design poiché il compito del Titolare sarà quello di adottare e attuare misure tecniche organizzative che tutelano i principi di protezione dei dati sin dal momento della progettazione. Differente è invece la Privacy by Default (art. 25 comma 2), il cui principio è quello di garantire che vengano trattati per impostazione predefinita solo i dati necessari per ogni specifica finalità del trattamento, garantendo in questo modo automaticamente il principio di minimizzazione dei dati;

5) «profilazione»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

6) «pseudonimizzazione»: il trattamento dei dati personali in modo tale che tali dati non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

7) «archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

8) «titolare del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

9) «responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

10) «destinatario»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali

nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri (4.5.2016 L 119/33 Gazzetta ufficiale dell'Unione europea IT) non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

11) "Responsabile della Protezione dei Dati Personali": noto con l'acronimo inglese DPO (Data Protection Officer), è la figura prevista e normata dagli artt. 37, 38 e 39 del Regolamento il cui compito precipuo è quello di monitorare il rispetto della normativa; fungere da *trait d'union* tra l'azienda ed il Garante; informare e fornire consulenza al titolare, al responsabile e/o ai dipendenti in ordine agli obblighi previsti dal Regolamento; fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati e sorvegliarne lo svolgimento;

12) «terzo»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

13) «consenso dell'interessato»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

14) «violazione dei dati personali» (Data Breach): la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

15) «dati biometrici»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

16) «dati relativi alla salute»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

17) «rappresentante»: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;

18) «impresa»: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;

19) «autorità di controllo»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51; (4.5.2016 L 119/34 Gazzetta ufficiale dell'Unione europea IT);

20) «obiezione pertinente e motivata»: un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al

presente regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione.

1.4. Qualità e conservazione dei dati personali, principio di necessità del trattamento

I dati personali devono essere:

- esatti ed aggiornati;
- trattati unicamente per gli scopi determinati, espliciti e legittimi definiti dalla Società;
- pertinenti, completi e non eccedenti rispetto alle finalità della raccolta.

I sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità. All'uopo sono utilizzate opportune clausole contrattuali, seguendo le procedure interne, le indicazioni del titolare e le indicazioni in termini di legge, quando lo sviluppo del software è commissionato all'esterno della Società. I dati personali da questa trattati sono conservati per il tempo necessario al raggiungimento delle finalità specificate nelle informative per le diverse categorie di soggetti, dopodiché vengono cancellati seguendo le procedure interne e le prescrizioni di legge.

1.5. Adempimenti

NOMINA DEL DPO: il Responsabile della Protezione dei dati deve essere nominato obbligatoriamente nei casi in cui, ex art. 37 del GDPR, le attività principali del Titolare consistano in trattamenti che, per la loro natura, ambito di applicazione e/o finalità, richiedano il monitoraggio regolare e sistematico degli interessati su larga scala; e tali attività consistano nel trattamento, su larga scala, di categorie particolari di dati.

CUP 2000 S.c.p.A. in data 21/05/2018 ha provveduto a nominare, con atto a firma dell'Amministratore Unico, il proprio DPO nella persona dell'Avv. Paolo Recla, comunicandone, per l'effetto, la designazione al Garante per la Protezione dei Dati Personali in data 25/05/2018 e pubblicandone i dati di contatto sul proprio sito web istituzionale (art. 37.7 del GDPR). Il Responsabile della protezione dei dati personali, *ex lege*, riferisce direttamente al vertice aziendale.

NOTIFICAZIONE DEI DATA BREACHES: ogni qual volta si verifichi un attacco informatico, una perdita, una manomissione o un accesso abusivo dei dati personali trattati il Titolare o, quando necessario, il Responsabile della Protezione dei dati deve avvertire l'Autorità di Controllo entro 72 ore dalla scoperta (art. 33). La notifica deve contenere le caratteristiche della violazione; il numero degli interessati coinvolti; i contatti interni dell'operatore (in

particolare quello del DPO) ed una stima delle conseguenze. Nel caso in cui tale violazione metta a rischio i diritti e le libertà degli interessati il Titolare dovrà, con un linguaggio semplice, informarli di quanto accaduto e delle misure adottare per affrontare la violazione.

INFORMARE I SOGGETTI INTERESSATI: Per questo gruppo di adempimenti sono considerate le categorie di soggetti interessati rappresentate dalle terze parti, persone fisiche, i cui dati sono trattati dalla Società. Sono altresì prese in considerazione le specifiche situazioni relative alla videosorveglianza con registrazione immagini, e ai trattamenti effettuati attraverso il sito internet.

NOMINARE, FORMARE E FORNIRE ISTRUZIONI AGLI AUTORIZZATI DEL TRATTAMENTO: l'Autorizzato del Trattamento è la persona fisica autorizzata dal Titolare o dal Responsabile a compiere le operazioni di trattamento dei dati. Avendo il compito di effettuare materialmente le operazioni di trattamento sui dati personali, egli deve agire sotto la diretta autorità del titolare del trattamento. Gli autorizzati sono nominati con apposito atto a firma del Direttore Generale pro tempore in qualità di Delegato alla gestione della privacy aziendale da parte del legale rappresentante (da ultimo, giusta determinazione n. 1 dell'Amministratore Unico in data 15 giugno 2017).

NOMINARE E FORNIRE ISTRUZIONI AI RESPONSABILI DEL TRATTAMENTO: i Responsabili elaborano i dati personali per conto del Titolare del trattamento nel pieno rispetto delle disposizioni in materia di protezione dei dati e delle linee guida del Titolare. La nomina a Responsabile del trattamento ex art. 28 del GDPR spetta al legale rappresentante della Società.

NOMINARE E ISTRUIRE GLI AMMINISTRATORI DI SISTEMA: l'amministratore di sistema o, tecnico sistemista di rete, è una figura professionale che approfondisce le competenze di un tecnico hardware e software soprattutto per quanto riguarda le caratteristiche delle architetture informatiche, i livelli di sistemistica e, in particolare, l'utilizzo e la condivisione di grandi quantità di dati attraverso le reti di comunicazione.

1.6. Responsabilità interna dei trattamenti, la struttura della funzione Privacy

La società, in qualità di Titolare del trattamento di dati personali, ha individuato la propria struttura di presidio della privacy che fa capo alla Direzione Generale, come precisato al successivo punto 1.6.2.

1.6.1. Titolare del trattamento

Il Titolare del trattamento ai sensi dell'art. 4, c.1, n. 8 del Regolamento europeo 2016/679 è la Società nel suo complesso, che è attualmente rappresentata dall' Amministratore Unico pro tempore, in qualità di Legale Rappresentante.

1.6.2. Delegato alla gestione della privacy

Con Determinazione dell'Amministratore Unico di CUP 2000 n. 1 del 15 giugno 2017, al Direttore Generale è stata delegata, previa sottoscrizione di apposita procura speciale, 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.

Il Delegato alla gestione della privacy ha la competenza esclusiva del riscontro rispetto alle richieste - da chiunque pervenute anche ai sensi dell'art. 15 del GDPR - di accesso, ovvero estrazione di dati di titolarità di CUP 2000, nonché di dati trattati da CUP 2000 in qualità di Responsabile del trattamento.

1.6.3. Area Affari Legali, Societari, Bandi e Appalti

Il Direttore Generale è supportato dalla Area Affari Legali, Societari, Bandi e Appalti (di seguito Ufficio Affari Legali) 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. 15 e ss. del Regolamento); cura gli approfondimenti normativi e verifica, con la collaborazione dell'Area Gestione Risorse Umane e dei Responsabili delle Divisioni aziendali, l'applicazione del presente regolamento e di ogni ulteriore disposizione aziendale in materia di privacy, ivi inclusa la corretta preposizione di Autorizzati 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. 1.6.5).

1.6.4. Responsabili del trattamento

Ai sensi dell'art. 28 del Regolamento, 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 presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento. 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.

1.6.5. Amministratori di sistema

Il Direttore Generale pro tempore, delegato alla gestione ed organizzazione della privacy interna alla società, giusta Determina del legale rappresentante (da ultimo, si veda la Determina sopra citata dell'Amministratore Unico di CUP 2000 in data 15/06/2017), individua gli Amministratori di Sistema – cui affidare gli adempimenti in materia di sicurezza indicati dal Regolamento all'art. 32 - tra il personale interno dotato di competenze tecniche in ottemperanza al 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), come modificato ed integrato dal successivo provvedimento del 25 giugno 2009.

Sulla base di tale valutazione, alla data di redazione del presente documento, 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 (ora Responsabile della Divisione DataCenter & Cloud) e i componenti del gruppo di lavoro che eroga servizi sistemistici all'interno della medesima Divisione.

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.

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 Divisione):

a) gestire le credenziali di autenticazione dei responsabili e dei soggetti autorizzati al trattamento/addetti alla manutenzione;
b) gestire i profili di autorizzazione degli autorizzati 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 autorizzato 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 fornitori di strumenti elettronici e di addetti esterni alla gestione e manutenzione di strumenti elettronici:

a) l'hardware sia conforme alla normativa in materia di protezione dei dati personali;
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;
   - la tracciabilità delle attività degli utenti, nel rispetto del Regolamento UE 2016/679 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 attuare al fine di una corretta gestione della privacy aziendale (Responsabile di Divisione):

a) verificare l'adozione delle misure adeguate 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 autorizzati al 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 Regolamento UE 2016/679;
h) comunicare a tutti gli autorizzati al 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 autorizzati/addetti, al conseguente eventuale aggiornamento dei profili attivi e, più in generale, sullo stato della sicurezza informatica aziendale.

Il Responsabile Divisione DataCenter & Cloud, 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 Autorizzati/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.

1.6.6. Autorizzati al trattamento (art. 29 e 4.10 del GDPR)

Gli autorizzati al trattamento sono i soggetti – nominati dal Titolare e/o dal Responsabile del trattamento (Art. 29 del Regolamento) – 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 nomina sottoscritta dal Direttore Generale; i nominativi degli Autorizzati al trattamento sono forniti all'Area Affari Legali dalle Divisioni aziendali, in accordo con l'Area Gestione Risorse umane, unitamente all'indicazione dell'ambito del trattamento.

1.7. Trattamenti affidati all'esterno della Società

Ricadono in questa fattispecie le esternalizzazioni di attività aziendali che comportano il trattamento di dati personali di cui la Società risulti essere Titolare del trattamento. È importante considerare che in tali situazioni deve essere prestata particolare attenzione al rapporto che si instaura con il destinatario dei dati. Nel caso in cui il destinatario sia un outsourcer di servizi, la normativa sulla privacy evidenzia obblighi specifici di controllo da parte del Titolare su tali trattamenti. Nel caso di designazione della società esterna quale responsabile del trattamento è richiesta, ad esempio, una fase propedeutica di valutazione dell'affidabilità del soggetto[1], la resa di specifiche istruzioni[2] ed il controllo dell'operato dell'outsourcer[3].

1.7.1. Esclusioni dalle operazioni di trattamento

Gli addetti alle pulizie appartenenti ad altre società, che, per necessità operative, accedono ai locali della Società, non sono autorizzati a svolgere alcuna operazione di trattamento. Gli autorizzati adottano comportamenti atti ad evitare che ai trattamenti da loro svolti accedano, pur se accidentalmente, le persone non autorizzate.

1.8. Dettaglio degli adempimenti

Le seguenti prescrizioni sono da intendersi VINCOLANTI per i dipendenti della Società che siano preposti in qualità di autorizzati del trattamento/addetti alla manutenzione e gestione.

SANZIONI ED ISPEZIONI: l'eventuale violazione delle disposizioni di seguito riportate costituisce un illecito, che può comportare l'applicazione di sanzioni di natura disciplinare ma anche di natura amministrativa e penale, secondo quanto previsto dal Regolamento 679/2016 e dal Codice Privacy integrato con le modifiche del D. Lgs. 101/2018 recante *Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonchè alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)*. 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 autorizzati 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] Se designato, il responsabile è individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

[2] I compiti affidati al responsabile sono analiticamente specificati per iscritto dal titolare.

[3] Il responsabile effettua il trattamento attenendosi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di cui al comma 2 e delle proprie istruzioni.

1. Ciascun autorizzato è tenuto a rispettare i principi generali previsti dal *Regolamento 679/2016*, con particolare riferimento alla liceità e correttezza del proprio agire: l'autorizzato può lecitamente effettuare le operazioni di trattamento secondo le modalità e le finalità espressamente stabilite per ciascun ambito di trattamento, 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 autorizzati, come previsto *dagli artt. 5-6 del Regolamento 2016/679*.
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 (ora "particolari" ex art. 9 del GDPR) 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 autorizzato/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. 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 autorizzato 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. 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 le 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.
7. Qualora l'autorizzato utilizzi, nello svolgimento delle proprie mansioni, atti/documenti contenenti dati personali comuni o particolari, 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.

8. 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.
9. I preposti alla duplicazione di documentazione (con stampanti o fotocopiatrici o altre periferiche) ovvero che utilizzino 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.

1.8.1. Richiesta di verifica preliminare

Il trattamento dei dati diversi da quelli particolari (art. 9) e quelli relativi a condanne penali e reati (art. 10) che presenta rischi specifici per i diritti e le libertà fondamentali è ammesso nel rispetto di misure ed accorgimenti a garanzia dell'interessato che sono prescritti dal Garante nell'ambito di una verifica preliminare anche a seguito di una richiesta del Titolare.

La verifica preliminare è da richiedere, ad esempio, per l'uso di sistemi di videosorveglianza c.d. "intelligenti", che non si limitano a riprendere e registrare le immagini, ma sono in grado di rilevare automaticamente comportamenti o eventi anomali, segnalarli, ed eventualmente registrarli.
Si dà atto che CUP 2000, in attuazione dei principi di necessità, proporzionalità e dei criteri di pertinenza e non eccedenza, utilizza per le proprie sedi aziendali impianti di videosorveglianza configurati in modo da raccogliere esclusivamente i dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando le sole immagini indispensabili, limitando l'angolo visuale delle riprese senza prevedere ingrandimenti e/o dettagli (si rinvia al *Regolamento per la disciplina e l'utilizzo degli impianti di videosorveglianza di CUP 2000* pubblicato sul sito istituzionale della società).

1.8.2. Informativa e consenso – Artt. 12, 13 e 14 del GDPR

Solo ed esclusivamente per i dati di cui CUP 2000 risulti Titolare.

All'atto della raccolta dei dati vi è l'obbligo di rendere l'informativa ai soggetti interessati e di raccogliere il consenso, ove necessario. La Società, di norma, acquisisce il consenso in forma scritta mediante apposita modulistica.

In conseguenza di quanto sopra, il trattamento dei dati personali può essere effettuato esclusivamente per le finalità riportate nelle informative suddette e, nel caso di necessità di consenso, solo per quelle finalità per le quali è stato rilasciato il consenso dagli interessati in conformità all'art. 7 del GDPR: è vietato qualsiasi altro utilizzo non esplicitamente compreso in tale consenso.

1.9. Riscontro delle richieste avanzate dagli interessati ai sensi dell'art. 15 del GDPR (Diritto d'accesso)

Il Regolamento tutela l'Interessato riservandogli, tra l'altro, specifici diritti (artt. da 15 a 22 del GDPR) in merito al trattamento ed al diritto di accesso ai propri dati personali e, in particolare, consentendo di ottenere dal Titolare, dal Responsabile, se designato, e/o dal DPO:

A. la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, la loro comunicazione in forma intelligibile nonché l'indicazione della loro origine, delle finalità e delle modalità del trattamento, della logica applicata in caso di trattamenti effettuati con l'ausilio di mezzi elettronici, degli estremi identificativi del Titolare, del Responsabile dei Trattamenti, del Responsabile della Protezione dei Dati Personali e del Rappresentante del Titolare, se designato, dei soggetti o delle categorie di soggetti che possono venirne a conoscenza dei propri dati personali;
B. l'aggiornamento, la rettifica, l'integrazione dei dati, la cancellazione, la trasformazione in forma anonima, il blocco dei dati trattati e l'attestazione che queste ultime operazioni (dall'aggiornamento al blocco) sono state portate a conoscenza di coloro ai quali i dati sono stati comunicati o diffusi; di opporsi in tutto o in parte per legittimi motivi al trattamento di dati personali che lo riguardano anche quando questo è previsto a fini di informazioni commerciali o di invio di materiale pubblicitario o di vendita diretta ovvero per il compimento di ricerche di mercato o di comunicazione commerciale.

L'interessato, inoltre, ha il diritto di proporre reclamo all'Autorità di Controllo.

Il riscontro alla richiesta dell'Interessato, ai sensi dell'art. 15 del Regolamento ("Diritto di accesso dell'Interessato"), deve essere effettuato dal Titolare o dal Responsabile.

Per l'esercizio dei suddetti diritti da parte dell'interessato la Società mette a disposizione apposito modello (Allegato 1) secondo il template formulato dal Garante della Protezione dei Dati Personali.

1.10. Nomina degli Autorizzati e ambito di trattamento consentito (art. 29 del GDPR)

La nomina degli autorizzati è un adempimento fondamentale per il trattamento dei dati personali sia in caso di utilizzo di strumenti elettronici[4] sia nel caso di trattamenti effettuati senza l'ausilio di essi[5].

Gli Autorizzati sono nominati dal Direttore Generale *pro tempore*, tramite una lettera di nomina:

[4] "Il trattamento di dati personali con strumenti elettronici è consentito agli autorizzati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti."

[5] Agli autorizzati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali".

- nel caso di nuovo dipendente, all'atto dell'assunzione o della specifica lettera di incarico alla mansione;
- nel caso di collaboratore esterno, all'inizio del rapporto di collaborazione;
- nel caso di *stagiaire,* all'inizio dello stage.

In tutti i suddetti casi la nomina ad autorizzato, corredata da specifiche istruzioni per l'ambito di trattamento assegnato, viene controfirmata in calce dal soggetto designato per ricevuta ed integrale presa visione.

1.10.1. Nomina degli Autorizzati del trattamento interni all'azienda (dipendenti e professionisti)

Il personale dipendente in servizio presso la Società è autorizzato a trattare i dati personali, di cui la Società è Titolare o Responsabile, strettamente necessari e/o comunque connessi alle funzioni proprie dell'unità organizzativa di appartenenza alla quale il singolo autorizzato è addetto. Tale trattamento può essere effettuato attraverso l'accesso agli archivi cartacei a disposizione della predetta unità organizzativa e l'utilizzo delle procedure informatiche previsto dal profilo di abilitazione assegnato.

I dati personali particolari e relativi a condanne penali, potranno essere trattati, nel rispetto delle Autorizzazioni generali emanate dall'Autorità Garante (in particolare le Autorizzazioni n. 1, 5 e 7) e reperibili sul sito della stessa Autorità, dalle seguenti categorie di autorizzati della Società:

- per quanto riguarda i dati inerenti il rapporto di lavoro dei dipendenti e assimilati e dei loro familiari: dagli addetti delle Risorse Umane, nonché dai diretti superiori;
- dati dei fornitori (che vengono acquisiti da Uffici/Enti certificatori Terzi e non dall'interessato): dall'Area Bandi & Appalti (ufficio legale);
- dati relativi a soggetti detenuti in relazione al progetto SISP (Sistema informativo/informatico a supporto delle attività sanitarie erogate ai soggetti detenuti negli Istituti Penitenziari della Regione Emilia Romagna) da parte dei dipendenti della società, appositamente preposti, che operano nell'ambito del progetto medesimo, nel rispetto degli atti di nomina formalizzati alla Società da parte delle Aziende sanitarie interessate.

Taluni autorizzati al trattamento di dati particolari e relativi a condanne penali o reati potranno ricevere ulteriori specifiche indicazioni che integrano quelle generali di cui alla presente Policy. I responsabili delle Unità Organizzative verificano periodicamente la pertinenza, non eccedenza e indispensabilità dei dati particolari e relativi a condanne penali o reati trattati presso le funzioni di competenza.

Inoltre, per quanto riguarda il personale addetto dell'Area Risorse Umane, del Servizio Internal Audit, e di IT in funzione del ruolo ricoperto, è consentito l'accesso ai dati di diversa natura (particolari, relativi a condanne penali, di rischio specifico), necessari allo svolgimento di detto ruolo.

In particolare, ciascun autorizzato del trattamento deve:

- rispettare i principi generali previsti dal Regolamento 2016/679, 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 essere 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'autorizzato, inoltre, deve:
- rispettare le misure adeguate di sicurezza adottate dalla società, atte a salvaguardare la riservatezza e l'integrità dei dati;
- 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.

1.10.2. Modalità di svolgimento delle operazioni: (modalità specifiche che riguardano solo alcuni autorizzati)

- Identificazione dell'autorizzato: 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'autorizzato, 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 particolare), 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.

1.10.3. Istruzioni per l'uso degli strumenti del trattamento

- **Strumenti elettronici:** ciascun autorizzato è responsabile del corretto utilizzo e della custodia degli strumenti elettronici in dotazione (a titolo esemplificativo

personal computer, periferiche, lettori di smart card, etc). 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;

- **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'autorizzato di individuare un proprio fiduciario autorizzato ad accedere alla casella assegnata dal titolare o dal responsabile del trattamento. Nell'ipotesi in cui la e-mail debba essere utilizzata per la trasmissione di dati particolari, 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 particolare;
    - nel corpo del messaggio sia presente un'intestazione standardizzata in cui si avverta della confidenzialità/riservatezza del messaggio;
- **distruzione delle copie cartacee:** coloro che sono preposti alla duplicazione di documentazione (con stampanti o fotocopiatrici o altre periferiche) ovvero che utilizzino 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;
- **atti e documenti cartacei:** gli atti e i documenti, contenenti dati personali o sensibili, non devono essere lasciati incustoditi; occorre che gli autorizzati, cui 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.

1.10.4. 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 autorizzato da parte di CUP 2000, è composta da un numero di caratteri almeno pari a otto o comunque pari al numero massimo di caratteri

consentito dal sistema. Ciascun autorizzato, nel gestire la propria password deve:

i. provvedere alla sostituzione immediata della password assegnata, secondo le modalità operative previste dal sistema, e successivamente cambiare la propria credenziale con cadenza almeno trimestrale;
ii. nel procedere alla sostituzione e al cambio periodico, ciascun autorizzato deve adottare una password di lunghezza almeno pari a quella che gli è stata precedentemente assegnata;
iii. scegliere una password che non deve contenere riferimenti agevolmente riconducibili alla sfera personale o all'identità dell'autorizzato medesimo;
iv. 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.

1.10.5. Misure di sicurezza

Le misure di sicurezza "adeguate" obbligatorie ex art. 32 del GDPR si differenziano a seconda della modalità del trattamento dei dati e pertanto sono di seguito individuate:

MISURE PER TRATTAMENTI EFFETTUATI CON STRUMENTI ELETTRONICI

Il trattamento di dati personali con strumenti elettronici è consentito agli autorizzati/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 autorizzati al 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 autorizzato, anche se in tempi differenti;
- Gli strumenti di autenticazione (password, dispositivi smart card ecc..) devono essere mantenuti riservati 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'-autorizzato/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'autorizzato;
  - 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' autorizzato al primo utilizzo e, successivamente, deve essere sostituita ogni 3 mesi (in caso consenta l'accesso a dati particolari) e comunque secondo le indicazioni ricevute;
  - Non includere la password in processi di connessione automatica;
  - Qualora una password perda di segretezza, l'autorizzato provvede immediatamente alla sua sostituzione.
- Gli eventuali dispositivi di autenticazione forniti in possesso ed uso esclusivo dell'autorizzato devono essere custoditi con cura e diligenza;
- Nel caso in cui la sessione di lavoro sia interrotta, l'autorizzato 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 autorizzato 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'autorizzato di individuare un proprio fiduciario autorizzato ad accedere alla casella assegnata dal titolare o dal responsabile del trattamento. Nell'ipotesi in cui la e-mail debba essere utilizzata per la trasmissione di dati particolari, 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.

Si raccomanda di prediligere, ove possibile la trasmissione "protetta" a mezzo posta elettronica certificata o, in subordine, a mezzo posta ordinaria con selezione, in questo caso, dell'opzione di "conferma di lettura" da parte del destinatario.

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 autorizzati 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 particolari o relativi a condanne penali o reati (artt. 9 e 10 del GDPR) 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 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 autorizzati 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' autorizzato, 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 particolari o relativi a condanne penali o reati (artt. 9 e 10 del GDPR) 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.

1.11. Change Management/Gestione dei Cambiamenti

La Gestione dei Cambiamenti delle applicazioni e risorse IT ha per obiettivo di garantire il controllo su modifiche, sostituzioni e adeguamenti ai sistemi.

Il processo presuppone:

- la predisposizione e il costante aggiornamento nel tempo di un inventario o mappa del patrimonio IT (hardware, software, dati);
- la valutazione dell'impatto dei cambiamenti sul sistema e dei rischi correlati con le proposte di modifica;
- attività di collaudo e test.

ALLEGATI

1) Modello - Istanza di accesso ai dati personali;
2) Modello - Istanza di accesso a videoregistrazioni.

L'Amministratore Unico
Dott. Alessandro Saccani
(sottoscritto con firma digitale)