CARBOSULCIS SpA

# REGOLAMENTO AZIENDALE SULLA PROTEZIONE DEI DATI PERSONALI

Applicazione del Regolamento Europeo 679/2016 ("GDPR"), del D.Lgs. 196/2003 come modificato e novellato dal D.Lgs. 101/2018

| | | | |
|---|---|---|---|
| Nome documento:<br>Data emissione: | **Regolamento interno privacy**<br>30/06/2020 | Versione<br>del | 01.01<br>21/10/2020 |
| Redatto da: | **Data Protection Officer** | Verificato ed approvato da: | **Titolare del trattamento - *Direzione Generale*** |
| Firma RPD/DPO | Pesupali Nicola | Firma | |

# SOMMARIO

PARTE PRIMA: INTRODUZIONE ..... 4

**1.** Premessa di carattere normativo ..... 4

**2.** Premessa di carattere organizzativo ..... 4

**3.** Premessa di carattere metodologico ..... 5

PARTE SECONDA: DISPOSIZIONI GENERALI ..... 6

**4.** Oggetto del Regolamento ..... 6

**5.** Finalità del Regolamento ..... 6

**6.** Sensibilizzazione ..... 6

**7.** Definizioni ..... 7

**8.** Principi applicabili al trattamento dei dati ..... 8

**9.** Trattamento di categorie particolari di dati ex art. 9 (c.d. dati sensibili) ..... 9

**10.** Trattamento dei dati personali relativi a condanne penali e reati ex art. 10 (c.d. dati giudiziari) ..... 10

**11.** Comunicazione di dati verso l'esterno ..... 10

PARTE TERZA: DIRITTI DELL'INTERESSATO ..... 11

**12.** Informativa sul trattamento dei dati ..... 11

**13.** Consenso al trattamento dei dati: principi generali ..... 12

**14.** Diritto di accesso dell'interessato ..... 12

**15.** Diritto di rettifica ..... 15

**16.** Diritto alla cancellazione (Diritto all'Oblio) ..... 15

**17.** Diritto di limitazione al trattamento ..... 15

**18.** Diritto alla portabilità dei dati ..... 15

**19.** Diritto di opposizione ..... 16

**20.** Processo decisionale automatizzato (Profilazione) ..... 16

PARTE QUARTA: TITOLARE E RESPONSABILE DEL TRATTAMENTO ..... 17

**21.** Titolare del trattamento ..... 17

**22.** Contitolari del trattamento ..... 18

**23.** Delegato/Designato al trattamento dei dati ..... 18

**24.** Responsabile del trattamento dei dati ..... 19

**25.** Autorizzato al trattamento dei dati ..... 21

**26.** Responsabile della Protezione dei Dati / Data Protection Officer (RPD/DPO) ..... 22

PARTE QUINTA: SICUREZZA DEI DATI PERSONALI - MISURE DI CARATTERE INFORMATICO E TECNOLOGICO ..... 24

**27.** Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita (Privacy by Design e Privacy by Default) ..... 24

**28.** Registro delle attività di trattamento ..... 24

**29.** Protezione e sicurezza dei dati personali ..... 24

**30.** Notifica di una violazione dei dati personali all'autorità di controllo (Data Breach) ..... 25

**31.** Valutazione di Impatto sulla Protezione dei Dati (DPIA) ..... 25

**32.** Trasferimento di dati personali all'estero ..... 26

**33.** Disciplina aziendale sulla videosorveglianza ..... 26

**34.** Disciplina aziendale sull'utilizzo dei mezzi informatici e telematici ..... 26

PARTE SESTA: ATTUAZIONE IN ..... AMBITO AZIENDALE 27

**35.** ENTRATA IN VIGORE E PUBBLICITÀ ..... 27

**36.** Disposizione finale relativa agli 'allegati tecnici' ..... 27

ALLEGATI AL PRESENTE REGOLAMENTO ..... 27

A. REGOLE PER L'ADOZIONE DELLE MISURE DI SICUREZZA ..... 28

B. DISCIPLINARE PER L'UTILIZZO DELLA RETE INFORMATICA ..... 31

C. DISCIPLINARE PER L'AUTORIZZATO AL TRATTAMENTO ..... 37

D. ISTRUZIONI OPERATIVE SULLE CORRETTE MODALITÀ DI UTILIZZO DEGLI STRUMENTI IN SMART WORKING ..... 39

# PARTE PRIMA: INTRODUZIONE

## 1. Premessa di carattere normativo

Il presente Regolamento in materia di protezione dei dati personali (c.d. "privacy") è uno strumento di applicazione del Decreto Legislativo 30 giugno 2003, n. 196 (cosiddetto "Codice sulla privacy") come novellato dal Decreto Legislativo 10 agosto 2018, n. 101 e, in particolare, del Regolamento Europeo n. 2016/679 (c.d. GDPR), nell'ambito dell'organizzazione della CARBOSULCIS SPA, con sede legale in Località Monte Sinni (Nuraxi Figus) - 09010 Gonnesa (Carbona-Iglesias/CI) – Sardegna/Italy.

Dal 25 maggio 2018 ha trovato diretta applicazione, sul territorio nazionale ed europeo, il nuovo Regolamento Europeo, approvato il 27 aprile 2016 e pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il 04 maggio 2016. Il Regolamento disciplina la protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché la libera circolazione di tali dati. Esso abroga la precedente Direttiva 95/46/CE.

In data 19/09/2018 è entrato in vigore il Decreto legislativo 10 agosto 2018, n. 101 che adegua il Codice in materia di protezione dei dati personali (Decreto legislativo 30 giugno 2003, n. 196) alle disposizioni del Regolamento (UE) 2016/679.

È necessario pertanto, come Azienda, dotarsi di un apposito "Regolamento" che disciplini compiti, attività e policy interne che garantiscano l'assolvimento degli adempimenti imposti dalle norme europee e nazionali.

Il presente Regolamento aziendale si rende inoltre necessario per recepire, in un unico testo, i precetti normativi di maggior rilevanza, sia di carattere aziendale che nazionale in tema di trattamento dei dati personali (D.lgs. 196 del 30/06/2003 e ss.mm., regolamenti e codici deontologici succeduti negli ultimi anni, direttive e linee guida del Garante, Direttiva dell'UE 2000/58 sulla riservatezza nelle comunicazioni elettroniche e soprattutto Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27/04/2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati).

Il presente Regolamento è sottoposto ad aggiornamento periodico, in linea con le novità normative, giurisprudenziali e con le pronunce del Garante per la protezione dei dati personali e organi simili.

## 2. Premessa di carattere organizzativo

Un'attenta disamina della normativa vigente in materia di privacy ha fatto emergere una necessità imprescindibile di cambiamento della mentalità che porti alla piena tutela della stessa, da considerare non solo come un oneroso rispetto di adempimenti burocratici, ma, soprattutto, come garanzia, per il cittadino-utente che si rivolge all'Azienda, di una completa riservatezza sotto il profilo sostanziale.

Il diritto alla protezione dei dati personali costituisce, anche secondo il Legislatore europeo, un vero e proprio diritto inviolabile dell'essere umano, che non si limita alla tutela della riservatezza o alla protezione dei dati, ma implica il pieno rispetto dei diritti e delle libertà fondamentali nonché dignità del singolo individuo. Per questi motivi, la "cultura della privacy" necessita di divenire un vero e proprio elemento cardine dell'organizzazione di questo Ente. A tale scopo è necessario che la CARBOSULCIS per mezzo del proprio personale si adoperi affinchè possa crescere e rafforzarsi una maggiore

consapevolezza in materia e ciò, non solo con una conoscenza minima dei principi fondamentali che stanno alla base della vigente normativa nel trattamento dei dati, ma anche ponendo in essere tutti gli adempimenti di carattere tecnico ed organizzativo per contribuire concretamente al miglioramento della qualità del rapporto con l'utenza ed implementare il "processo di umanizzazione".

## 3. Premessa di carattere metodologico

Vengono allegati a questo Regolamento una serie di documenti tecnici atti a dare compiuta attuazione ai dettami della nuova "privacy europea".

Tali documenti, ai quali viene data massima pubblicità e diffusione tramite la pubblicazione sul sito internet (e intranet) aziendale, sono:

A. Regole per l'adozione delle misure di sicurezza;

B. Disciplinare per l'uso della rete informatica;

C. Disciplinare per l'autorizzato al trattamento;

D. Procedura per la gestione delle violazioni – c.d. "Data Breach".

Si sottolinea come il principio cardine della "***Responsabilizzazione***" (accountability nell'accezione anglosassone), introdotto dal GDPR, imponga al Titolare del trattamento dei dati l'obbligo di attuare delle politiche adeguate in materia di protezione dei dati, con l'adozione di misure tecniche ed organizzative, anche certificate, che siano concretamente e sempre dimostrabili, oltre che conformi alle disposizioni europee (principio della "conformità" o ***compliance*** nell'accezione inglese); e ciò anche attraverso dei comportamenti proattivi, atti a dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del Regolamento.

La normativa vigente lascia al Titolare ampia autonomia decisionale in merito alle modalità, alle garanzie e ai limiti del trattamento dei dati personali, nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel Regolamento.

Pertanto questa Azienda si sta impegnando, a far proprio i dettami del Legislatore europeo relativo all'accountability ed alla compliance. anche attraverso la predisposizione di questo documento.

# PARTE SECONDA: DISPOSIZIONI GENERALI

## 4. Oggetto del Regolamento

Il presente Regolamento disciplina, all'interno dell'Ente, la tutela delle persone in ordine al trattamento dei dati personali, nel rispetto di quanto previsto dal Codice in materia di protezione dei dati personali (Decreto Legislativo del 30/06/2003 n. 196 e ss.mm.ii.) ed in conformità all'emanazione della nuova normativa sovranazionale, il Regolamento UE n. 679 del Parlamento Europeo e del Consiglio del 27/04/2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

## 5. Finalità del Regolamento

L'Azienda garantisce che il trattamento dei dati, a tutela delle persone fisiche, si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali, a prescindere dalla nazionalità o dalla residenza dell'interessato.

La protezione delle persone fisiche, con riguardo al trattamento dei dati personali, è un diritto fondamentale. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano (articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione Europea.)

## 6. Sensibilizzazione

La Carbosulcis sostiene e promuove, al suo interno, ogni strumento di sensibilizzazione che possa consolidare il pieno rispetto del diritto alla riservatezza e migliorare la qualità del servizio offerto agli utenti/clienti.

A tale riguardo, uno degli strumenti essenziali di sensibilizzazione, anche in materia di privacy, è l'attività formativa del personale aziendale e l'attività informativa diretta a tutti coloro che hanno rapporti con l'Azienda.

Per garantire la conoscenza capillare delle disposizioni introdotte dal nuovo Regolamento europeo, e di conseguenza contenute nel presente Regolamento aziendale, al momento dell'ingresso in servizio è fornita, a cura dell'Ufficio Personale, ad ogni dipendente (oltre che ad ogni collaboratore, consulente o titolare di borsa di studio) una specifica comunicazione in materia di privacy, con apposita clausola inserita nel contratto di lavoro (o nella lettera di incarico per i soggetti non dipendenti poc'anzi citati), con la quale detti soggetti (dipendenti e non dipendenti) sono nominati quali "Autorizzati al trattamento dei dati" e/o "Responsabili del trattamento" ai sensi rispettivamente degli articoli 29 e 28 del Regolamento UE 2016/679.

Il Regolamento, pubblicato sul sito aziendale, contiene infatti tutti i principi fondamentali della materia, esposti in maniera semplice, chiara e puntuale e il dipendente (o il non dipendente nei termini di cui si è detto sopra), nel sottoscrivere il contratto di lavoro (o la lettera di incarico), è reso edotto dell'esistenza dell'anzidetto Regolamento e delle modalità di consultazione del medesimo.

## 7. Definizioni

Come stabilito dall'articolo n. 4 del Regolamento Europeo n. 2016/679, ai fini di questo disciplinare aziendale si intende per:

a) «**dato personale** »: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può esser identificata, direttamente o indirettamente, con particolare riferimento a un identificativo 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;

b) «**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;

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

d) «**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;

e) «**pseudonimizzazione**»: il trattamento dei dati personali in modo tale che i dati personali 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;

f) «**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;

g) «**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 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;

h) «**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;

i) «**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;

l) «**violazione dei dati personali** »: 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;

m) «**dati genetici**»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

n) «**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;

o) «**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; a proposito delle tipologie di "dati" sopra indicate, si fa presente che il Regolamento europeo non utilizza la definizione "dati sensibili" per la quale, quanto meno sino all'emanazione della legge italiana di revisione del D.lgs. 196/20013, si fa espresso rinvio all'articolo n. 4 del vigente Codice della privacy (D.lgs. 196/2003): definizione che, quindi, al momento rimane nell'utilizzo e nel linguaggio corrente per la materia di cui si tratta.

p) «**autorità di controllo** »: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del Regolamento UE;

Quelle sopra riportate, di cui si è data evidenza, rappresentano le "definizioni" su cui ha inciso maggiormente il Regolamento europeo: per le altre "definizioni" si fa espresso rinvio al testo dell'articolo n. 4 del Regolamento Europeo n. 2016/679.

## 8. Principi applicabili al trattamento dei dati

Come stabilito dall'articolo n. 5 del Regolamento Europeo n. 2016/679, i dati personali sono:

a. trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);

b. raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1 del Regolamento UE, considerato incompatibile con le finalità iniziali («limitazione della finalità»);

c. adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»). A tale proposito, il Regolamento UE ricalca i principi sostanziali di "necessità, pertinenza, indispensabilità e non eccedenza" (rispetto alle finalità del trattamento) contenuti negli articoli 4 e 11 del D.lgs. 196/2003.

d. esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);

e. conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del Regolamento UE, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione »);

f. trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza »).

Come stabilito dal GDPR, il Titolare è competente per il rispetto di quanto sin qui esposto ed è in grado di comprovarlo verso l'esterno (principio europeo dell'«accountability» o «responsabilizzazione»).

## 9. Trattamento di categorie particolari di dati ex art. 9 (c.d. dati sensibili)

Come stabilito dall'articolo n. 9 del GDPR , è vietato trattare dati personali che rivelino l' origine razziale o etnica , le opinioni politiche, le convinzioni religiose o filosofiche , o l'appartenenza sindacale , nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona .

Detta disposizione non si applica, secondo il Regolamento UE, quando incorrono alcune condizioni, riportate al summenzionato articolo n. 9, tra le quali si evidenzia quella di cui alla lettera "e" applicabile a questo Ente, ai sensi della quale " il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato", nonché quella di cui alla lettera "b" e "c", applicabile a questo Ente, ai sensi della quale "il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso" e "il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento".

Si fa presente, inoltre, che il Regolamento UE consente di "mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute" (articolo n. 9, paragrafo n. 4). Posto quanto sopra, si fa rinvio alle vigenti disposizioni emanate, in materia di dati sensibili, biometrici e genetici e in particolare al "Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art.21, comma 1 del D.Lgs 10 Agosto 2018, n. 101" del Garante della Privacy, pubblicato in Gazzetta Ufficiale il 05 Giugno 2019.

## 10. Trattamento dei dati personali relativi a condanne penali e reati ex art. 10 (c.d. dati giudiziari)

Come stabilito dall'articolo n. 10 del Regolamento Europeo n. 2016/679 , "il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. *Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica."

Il Regolamento UE 2016/679 pertanto ravvisa quali condizioni necessarie per il trattamento su detto la presenza di una base giuridica che lo giustifichi (l'art. 6, paragrafo 1 del GDPR) ed altresì il controllo dell'autorità pubblica l'autorizzazione del diritto dell'Unione o degli Stati membri, nel rispetto delle garanzie appropriate per i diritti e le libertà degli interessati.

La dottrina prevalente, in merito al fondamento giuridico che consenta di trattare i dati relativi a condanne penali e reati per valutare l'attitudine lavorativa, ha ritenuto che l'autorizzazione da parte del diritto nazionale già risulti presente ai sensi dell'art. 8 del c.d. "Statuto dei Lavoratori" (L. 300/1970) che ne prevede il trattamento nell'ambito della valutazione dell'attitudine lavorativa.

## 11. Comunicazione di dati verso l'esterno

La comunicazione a soggetti terzi di dati di carattere personale e particolare, detenuti dal Titolare del Trattamento, deve avvenire unicamente in ragione delle finalità per le quali gli stessi sono stati acquisiti e di cui si è data contezza nell'informativa privacy consegnata agli interessati. *La diffusione di dati che ecceda quanto su indicato, deve considerarsi illecita.

L'eventuale comunicazione di dati particolari e giudiziari tra soggetti pubblici, è ammessa solo in presenza di una normativa o di un regolamento che la giustifichino e, in ogni caso, qualora risulti necessaria per lo svolgimento di funzioni istituzionali, anche a seguito di un bilanciamento degli interessi.

# PARTE TERZA: DIRITTI DELL'INTERESSATO

## 12. Informativa sul trattamento dei dati

Come stabilito dall'articolo n. 13 del Regolamento Europeo n. 2016/679, in caso di raccolta presso l'interessato di dati che lo riguardano, il Titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni:

a. l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;

b. i dati di contatto del Responsabile della Protezione dei Dati (RPD/DPO);

c. le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;

d. qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f) del Regolamento UE, i legittimi interessi perseguiti dal titolare del trattamento o da terzi;

e. gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;

f. ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione, nei termini previsti dal Regolamento UE.

In aggiunta alle informazioni di cui sopra, nel momento in cui i dati personali sono ottenuti, il titolare del trattamento fornisce all'interessato le seguenti ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente:

g. il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

h. l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;

i. qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a) del Regolamento UE, l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;

j. il diritto di proporre reclamo a un'autorità di controllo;

k. se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;

l. l'eventuale esistenza di un processo decisionale automatizzato , compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4 del Regolamento UE, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Per quanto concerne il periodo di conservazione dei dati personali raccolti da questo Ente, i dati verranno conservati in una forma che consenta l'identificazione dell'interessato per un periodo di

tempo non superiore a quello strettamente necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

Qualora il Titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità.

## 13. Consenso al trattamento dei dati: principi generali

Il GDPR conferma che ogni trattamento deve trovare fondamento in un'idonea base giuridica; i fondamenti di liceità del trattamento sono indicati all'art. 6 del GDPR.

In particolare:

- il consenso deve essere "esplicito" o il trattamento deve basarsi sul verificarsi dei casi previsti dal GDPR;
- deve essere, in tutti i casi, libero, specifico, informato e inequivocabile e non è ammesso il consenso tacito o presunto (non è quindi possibile utilizzare "caselle pre-spuntate" su un modulo);
- deve essere manifestato attraverso "dichiarazione o azione positiva inequivocabile" (per approfondimenti, si vedano considerando 39 e 42 del regolamento).

Il GDPR prevede tuttavia, sempre all'art. 6, ulteriori fattispecie in cui il trattamento è lecito, senza dover ricorrere al consenso. In particolare:

- il trattamento è necessario all' esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso. La sussistenza tra le parti di un contratto o di una fase pre- contrattuale rappresenta un rapporto basato su uno scambio di volontà tale da implicare tacitamente la volontà necessaria per il trattamento dati. Tale presupposto legittimante il trattamento va interpretato in senso restrittivo, solo qualora il trattamento sia una condizione necessaria alla corretta esecuzione degli adempimenti contrattuali e pre-contrattuali;
- il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare;
- il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento: si intende a prescindere dalla natura giuridica dell'Ente (pubblica o privata), purchè il compito sia di interesse della collettività;
- l'interesse legittimo prevalente di un titolare o di un terzo presuppone invece che sia il titolare stesso ad effettuare un bilanciamento fra il legittimo interesse suo o del terzo e i diritti e libertà dell'interessato e non sia più compito dell'Autorità. Pertanto l'interesse legittimo del titolare o del terzo deve risultare prevalente sui diritti e le libertà fondamentali dell'interessato per costituire un valido fondamento di liceità. Il regolamento chiarisce espressamente che l'interesse legittimo del titolare non costituisce idonea base giuridica per i trattamenti svolti dalle autorità pubbliche in esecuzione dei rispettivi compiti.

## 14. Diritto di accesso dell'interessato

Come stabilito dall'articolo n. 15 del Regolamento Europeo n. 2016/679, l'interessato ha il diritto di ottenere dal Titolare del trattamento la conferma che sia o meno in corso un trattamento di dati

personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:

a. le finalità del trattamento;

b. le categorie di dati personali in questione;

c. i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;

d. quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

e. l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;

f. il diritto di proporre reclamo a un'autorità di controllo;

g. qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;

h. l'esistenza di un processo decisionale automatizzato , compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Oltre al rispetto delle prescrizioni relative alle modalità di esercizio di questo diritto, il Titolare può consentire agli interessati di consultare direttamente, da remoto e in modo sicuro, i propri dati personali.

Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate ai sensi dell'articolo 46 relative al trasferimento.

Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento.

In caso di ulteriori copie richieste dall'interessato, il titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi. Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune.

Il diritto di ottenere una copia non deve ledere i diritti e le libertà altrui.

Per quanto riguarda, inoltre, le modalità concrete per mezzo delle quali trova attuazione, nell'attuale contesto normativo ed organizzativo, il diritto di accesso , si fa rinvio alle vigenti diposizioni normative e regolamentari emanate, negli anni, dal Legislatore statale nonché dal Garante per la privacy.

In questa Azienda, la competenza sulla materia de quo è affidata al Responsabile della Prevenzione della Corruzione e Trasparenza.

A tale riguardo, nel rinviare a quanto pubblicato al sito web aziendale, si fa presente che:

a. per accesso documentale si intende la domanda di accesso (richiesta di presa visione o di rilascio copia) a delibere e provvedimenti/atti dell'Azienda, nei termini e alle modalità previste dalla

normativa vigente (Legge 07 agosto 1990 n. 241 e ss.mm.ii.). Possono fare domanda tutti i cittadini portatori di un interesse "diretto, concreto e attuale, corrispondente ad una situazione giuridicamente tutelata e collegata al documento al quale è richiesto l'accesso" (art. 22, Legge 241/1990). Per presentare domanda, è necessario rivolgersi alla Carbosulcis, compilando un apposito modulo e portando con sé il proprio documento di identità valido. E' possibile altresì utilizzare la procedura informatizzata presente nella sezione "Amministrazione Trasparente" del sito istituzionale, seguendo le istruzioni ivi presenti. I costi di riproduzione e di ricerca/visura, sono stabiliti dall'Azienda con propria deliberazione. Il procedimento di accesso si conclude entro 30 giorni, decorrenti dalla presentazione della richiesta all'ufficio competente.

b. per accesso civico si intende il diritto di chiunque di richiedere documenti, informazioni o dati che le pubbliche amministrazioni non hanno pubblicato pur avendone l'obbligo (Decreto Legislativo 97 del 17/5/2016 "Revisione e semplificazione delle disposizioni in materia di prevenzione della corruzione pubblicità e trasparenza delle Amministrazioni Pubbliche" , e Decreto Legislativo 33 del 14/03/2013: "Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni"). La richiesta viene presentata al Responsabile della Prevenzione della Corruzione e della Trasparenza utilizzando il modulo prodotto sul sito internet aziendale. L'Azienda, entro 30 giorni, procede alla pubblicazione nel sito del documento, dell'informazione o del dato richiesto e lo trasmette contestualmente al richiedente, ovvero comunica al medesimo l'avvenuta pubblicazione, indicando il collegamento ipertestuale a quanto richiesto. Se il documento, l'informazione o il dato richiesti risultano già pubblicati nel rispetto della normativa vigente, l'Azienda indica al richiedente il relativo collegamento ipertestuale. Nei casi di ritardo o mancata risposta il richiedente può ricorrere al titolare del potere sostitutivo che, verificata la sussistenza dell'obbligo di pubblicazione, provvede alla pubblicazione nel sito del documento, dell'informazione o del dato richiesto e lo trasmette contestualmente al richiedente, ovvero comunica al medesimo l'avvenuta pubblicazione, indicando il collegamento ipertestuale a quanto richiesto.

c. per accesso generalizzato si intende il diritto di chiunque di accedere ai dati e ai documenti detenuti dalle Pubbliche Amministrazioni, ulteriori rispetto a quelli oggetto di pubblicazione ai sensi del Decreto Legislativo 33/2013 ('Decreto Trasparenza') e del D.lgs. 97/2016 (così detto Freedom of Information Act o "FOIA"), nel rispetto dei limiti relativi alla tutela di interessi giuridicamente rilevanti, allo scopo di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche e di promuovere la partecipazione al dibattito pubblico. La richiesta viene presentata all'Ufficio Relazioni con il Pubblico. Il procedimento di accesso generalizzato deve concludersi con provvedimento espresso e motivato nel termine d i 30 giorni dalla presentazione dell'istanza, con la comunicazione dell'esito al richiedente e agli eventuali contro interessati. Tali termini sono sospesi (fino ad un massimo di 10 giorni) nel caso di comunicazione della richiesta al controinteressato. Se il documento risulta già pubblicato nel sito aziendale nel rispetto della normativa vigente, l'Azienda indica al richiedente il relativo collegamento ipertestuale. Nei casi di diniego totale o parziale dell'accesso o di mancata risposta entro il termine indicato, il richiedente può presentare richiesta di riesame al Responsabile della Prevenzione della Corruzione e della Trasparenza, che decide con provvedimento motivato, entro il termine di 20 giorni. Se l'accesso è stato negato o differito il suddetto Responsabile provvede sentito il Garante per la protezione dei dati personali, il quale si pronuncia entro il termine di 10 giorni dalla richiesta. A decorrere dalla comunicazione al Garante, il

termine per l'adozione del provvedimento da parte del Responsabile è sospeso fino alla ricezione del parere del Garante e comunque per un periodo non superiore ai predetti 10 giorni. Avverso la decisione dell'amministrazione competente o, in caso di richiesta di riesame, avverso quella del Responsabile della Prevenzione della Corruzione e della Trasparenza, il richiedente può proporre ricorso al tribunale amministrativo regionale (TAR).

## 15. Diritto di rettifica

Come stabilito dall'articolo n. 16 del Regolamento Europeo n. 2016/679, l'interessato ha il diritto di ottenere dal Titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

## 16. Diritto alla cancellazione (Diritto all'Oblio)

Come stabilito dall'articolo n. 17 del Regolamento Europeo n. 2016/679, in capo all'interessato è riconosciuto il diritto "all'oblio", che si configura come un diritto alla cancellazione dei propri dati personali in forma rafforzata.

Si prevede, infatti, l'obbligo per i Titolari (se hanno "reso pubblici" i dati personali dell'interessato: ad esempio, pubblicandoli su un sito web) di informare della richiesta di cancellazione altri titolari che trattano i dati personali cancellati, compresi "qualsiasi link, copia o riproduzione" (si veda art. 17, paragrafo 2 del Regolamento UE).

## 17. Diritto di limitazione al trattamento

Si tratta di un diritto diverso e più esteso rispetto al "blocco" del trattamento di cui all'art. 7, comma 3, lettera a), del Codice: in particolare, è esercitabile non solo in caso di violazione dei presupposti di liceità del trattamento (quale alternativa alla cancellazione dei dati stessi), bensì anche se l'interessato chiede la rettifica dei dati (in attesa di tale rettifica da parte del titolare) o si oppone al loro trattamento ai sensi dell'art. 21 del regolamento (in attesa della valutazione da parte del titolare).

Esclusa la conservazione, ogni altro trattamento del dato di cui si chiede la limitazione è vietato a meno che ricorrano determinate circostanze (consenso dell'interessato, accertamento diritti in sede giudiziaria, tutela diritti di altra persona fisica o giuridica, interesse pubblico rilevante).

Il diritto alla limitazione prevede che il dato personale sia "contrassegnato" in attesa di determinazioni ulteriori; pertanto, è opportuno che il Titolare preveda nei propri sistemi informativi (elettronici o meno) misure idonee a tale scopo.

## 18. Diritto alla portabilità dei dati

Si tratta di uno dei nuovi diritti previsti dal GDPR, anche se non è del tutto sconosciuto ai consumatori (*si pensi alla portabilità del numero telefonico*).

Non si applica ai trattamenti non automatizzati (quindi non si applica agli archivi o registri cartacei) e sono previste specifiche condizioni per il suo esercizio ; in particolare, sono portabili solo i dati trattati con il consenso dell'interessato o sulla base di un contratto stipulato con l'interessato (quindi non si applica ai dati il cui trattamento si fonda sull'interesse pubblico o sull'interesse legittimo del

titolare, per esempio), e solo i dati che siano stati "forniti" dall'interessato al Titolare (si veda il considerando 68 del Regolamento UE).

Inoltre, il Titolare deve essere in grado di trasferire direttamente i dati portabili a un altro titolare indicato dall'interessato, se tecnicamente possibile.

## 19. Diritto di opposizione

Come stabilito dall'articolo n. 21 del Regolamento Europeo n. 2016/679, l'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f) del medesimo Regolamento, compresa la profilazione sulla base di tali disposizioni.

Il Titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

## 20. Processo decisionale automatizzato (Profilazione)

Come stabilito dall'articolo n. 22 del Regolamento Europeo n. 2016/679, l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato , compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.

Tale principio non si applica nel caso in cui la decisione:

- sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento;
- sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà dei legittimi interessi dell'interessato;
- si basi sul consenso esplicito dell'interessato.

# PARTE QUARTA: TITOLARE E RESPONSABILE DEL TRATTAMENTO

## 21. Titolare del trattamento

Il "Titolare" del trattamento dei dati personali è la persona fisica, persona giuridica, la Pubblica Amministrazione, e qualsiasi altro Ente, Associazione od organismo cui competono le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, compreso il profilo della sicurezza.

Il Titolare del trattamento dei dati personali, ai sensi e per gli effetti della vigente normativa è la Carbosulcis Spa ( "Titolare del trattamento" o "Titolare"), con sede in Località Monte Sinni "Nuraxi Figus" - 09010 Gonnesa (Carbona-Iglesias/CI) - P.IVA: 00456650928 - Centralino: 0781.4921__ - Fax: 0781.4922400 - E-mail: privacy@carbosulcis.eu - PEC: presidenza@pec.carbosulcis.eu.

Il Titolare, avvalendosi della supervisione e collaborazione del Data Protection Officer , provvede:

a) a richiedere al Garante per la protezione dei dati personali l'eventuale autorizzazione al trattamento dei dati personali, nei casi previsti dalla vigente normativa e ad assolvere all'eventuale obbligo di notificazione e comunicazione;

b) a designare con atto/contratto i Responsabili del trattamento dei dati personali, impartendo ad essi, per la corretta gestione e tutela dei dati personali, i compiti e le necessarie istruzioni, in relazione all'informativa agli interessati, alla tipologia dei dati da trattare, alle condizioni normative previste per il trattamento dei dati, alle modalità di raccolta, comunicazione e diffusione dei dati, all'esercizio dei diritti dell'interessato previsti all'articolo 12 e ss del GDPR, all'adozione delle misure di sicurezza per la conservazione, alla protezione e sicurezza dei dati;

c) a nominare il Data Protection Officer, come stabilito dall'articolo 37 del Regolamento UE;

d) a disporre periodiche verifiche sul rispetto delle istruzioni impartite, anche con riguardo agli aspetti relativi alla sicurezza dei dati;

e) a mettere in atto misure tecniche e organizzative adeguate a garantire che il trattamento dei dati sia effettuato conformemente al presente Regolamento.

Si dà evidenza, inoltre, del fatto che il Regolamento UE pone con forza l'accento sulla "responsabilizzazione" (accountability nell'accezione inglese) di titolari e responsabili, ovverossia sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento (si vedano artt. 23-25, in particolare, e l'intero Capo IV del Regolamento).

Si tratta di una grande novità per la protezione dei dati in quanto viene affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali, nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel regolamento.

Questa Ente sta lavorando attivamente per far proprio l'approccio del Legislatore europeo relativo all'accountability.

## 22. Contitolari del trattamento

Come stabilito dall'articolo n. 26 del Regolamento Europeo n. 2016/679, allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal GDPR, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni.

Tale accordo può designare un punto di contatto per gli interessati e riflette adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato.

Indipendentemente dalle disposizioni dell'accordo anzidetto, l'interessato può esercitare i propri diritti ai sensi del Regolamento UE nei confronti di e contro ciascun Titolare del trattamento.

## 23. Delegato/Designato al trattamento dei dati

Secondo la vigente normativa, s'intende per Responsabile del trattamento dei dati, "la persona fisica, giuridica, la Pubblica Amministrazione e qualsiasi altro Ente, Associazione ed Organismo preposti dal Titolare al trattamento di dati personali".

Anche se il Regolamento Europeo (art. 28) disciplina i compiti del Responsabile "esterno" senza contemplare espressamente la figura ed i compiti del Responsabile "interno", questo Ente, in considerazione della complessità e della molteplicità delle proprie funzioni istituzionali e della necessità di continuare a garantire, a tutti i livelli, la più efficace applicabilità dei precetti in materia di privacy, reputa necessario, [...]

anche ai sensi del Capo IV (Disposizioni relative al titolare del trattamento e al responsabile del trattamento) - Art. 2-quaterdecies (Attribuzione di funzioni e compiti a soggetti designati) del D.Lgs. 101/2018 che recita: - *1. Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità*';

[...] continuare a designare in ambito aziendale i Delegati/Designati al trattamento dei dati personali, conferendo l'incarico a quei dirigenti/Responsabili di P.O./ figure apicali che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate a far sì che il trattamento soddisfi i requisiti del presente Regolamento e garantisca la tutela dei diritti dell'interessato.

Il Titolare del trattamento dei dati deve informare ciascun Delegato/Designato al trattamento dei dati, così come individuato dal presente Regolamento, delle responsabilità che gli sono affidate in relazione a quanto disposto dalle normative vigenti. Essi rispondono al Titolare di ogni violazione o mancata attivazione di quanto dettato dalla normativa vigente.

Il Delegato/Designato del trattamento deve:

1. trattare i dati personali, anche particolari, osservando le disposizioni del presente Regolamento aziendale nonché le specifiche istruzioni impartite dal Titolare;

2. garantire che, presso la propria struttura, le persone autorizzate (incaricate) al trattamento dei dati personali assolvano ad un adeguato livello di riservatezza;

3. adottare idonee misure per garantire, nell'organizzazione delle prestazioni e dei servizi presso la propria struttura, il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati, nonché del segreto professionale, fermo restando quanto previsto dalla normativa vigente;

4. tenendo conto della natura del trattamento, assistere il Titolare del trattamento con misure tecniche ed organizzative adeguate, al fine di soddisfare l'obbligo del Titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato secondo quanto previsto nella normativa vigente;

5. mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi previsti nel presente Regolamento;

6. contribuire alle attività di verifica del rispetto del regolamento, comprese le ispezioni, realizzate dal titolare del trattamento o da altro soggetto da questi incaricato.

Il Delegato/Designato per il trattamento dei dati personali, nell'espletamento della sua funzione, deve inoltre collaborare con il Data Protection Officer (DPO) aziendale , al fine di:

a) comunicare al DPO, quando questi ne faccia richiesta, ogni notizia rilevante ai fini dell'osservanza degli obblighi dettati dagli articoli da 32 a 36 del Regolamento UE 2016/679 riguardanti: l'adozione di misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio; la notificazione di una violazione dei dati personali al Garante privacy; la comunicazione di una violazione dei dati personali all'interessato, la predisposizione del Registro dei trattamenti .

b) utilizzare il modello aziendale di Informativa e Consenso verificandone il rispetto e fornendo al DPO, quando questi ne faccia richiesta, le informazioni utili per l'aggiornamento del registro dei trattamenti;

c) rispondere alle istanze degli interessati e stabilire modalità organizzative volte a facilitare l'esercizio del diritto di accesso dell'interessato e la valutazione del bilanciamento degli interessi in gioco;

d) contribuire a far sì che tutte le misure di sicurezza riguardanti i dati dell'Azienda siano applicate all'interno dell'Azienda stessa ed all'esterno, qualora agli stessi vi sia accesso da parte di soggetti terzi quali Responsabili del trattamento;

e) informare il Titolare del trattamento, senza ingiustificato ritardo, della conoscenza dell'avvenuta violazione dei dati personali.

## 24. Responsabile del trattamento dei dati

Nell'ambito di questo Ente, sono inoltre individuati quali Responsabili del trattamento dei dati personali , tutti i soggetti esterni che, per svolgere la propria attività sulla base di una convenzione o un contratto/atto sottoscritto con l'Azienda, trattino dati di cui è titolare l'Ente medesimo e qualora siano in possesso dei requisiti previsti dall'articolo 28 del GDPR (esperienza, capacità ed affidabilità).

In ottemperanza all'articolo 28 del Regolamento Europeo 2016/679, i Responsabili hanno l'obbligo di:

- trattare i dati in modo lecito, secondo correttezza e nel pieno rispetto della vigente normativa (nazionale ed europea) in materia di privacy;

- trattare i dati personali, anche di natura sensibile e giudiziaria, degli utenti/clienti (o di altri interessati) esclusivamente per le finalità previste dal contratto o dalla convenzione stipulata con il Titolare e ottemperando ai principi generali di necessità, pertinenza e non eccedenza;

- rispettare i principi in materia di sicurezza dettati dalla normativa vigente (nazionale ed europea) in materia di privacy, idonei a prevenire e/o evitare operazioni di comunicazione o diffusione dei dati non consentite, il rischio di distruzione o perdita, anche accidentale, il rischio di accesso non autorizzato o di trattamento non autorizzato o non conforme alle finalità della raccolta;

- adottare, secondo la propria organizzazione interna, misure tecniche ed organizzative idonee a garantire un livello di sicurezza adeguato al rischio, nei termini di cui all'articolo 32 del Regolamento Europeo 2016/679 rubricato "Sicurezza del trattamento" che possono anche essere definite dal Titolare del Trattamento;

- nominare, al loro interno, i soggetti autorizzati al trattamento, impartendo loro tutte le necessarie istruzioni finalizzate a garantire, da parte degli stessi, un adeguato obbligo legale di riservatezza;

- attenersi alle disposizioni impartite dal Titolare del trattamento, anche nell'eventuale caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, nei termini di cui all'articolo 28, comma 3, lettera a) del Regolamento Europeo;

- specificare, su richiesta del Titolare, i luoghi dove fisicamente avviene il trattamento dei dati e su quali supporti e le misure minime di sicurezza adottate per garantire la riservatezza e la protezione dei dati personali trattati.

- assistere, per quanto di competenza e nella misura in cui ciò sia possibile, il Titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del Regolamento Europeo (sicurezza del trattamento dei dati personali, notifica di una violazione dei dati personali all'autorità di controllo, comunicazione di una violazione dei dati personali all'interessato, valutazione di impatto sulla protezione dei dati), tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;

- su scelta del Titolare del trattamento, cancellare o restituire al medesimo tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancellare le copie esistenti, salvo che il diritto dell'Unione o dello Stato membro preveda la conservazione dei dati;

- mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all'articolo 28 del Regolamento Europeo e consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzate dal Titolare del trattamento o da un altro soggetto da questi incaricato.

Nel caso di mancato rispetto delle predette disposizioni e in caso di mancata nomina dei soggetti autorizzati al trattamento dei dati ne risponde direttamente, verso il titolare, il Responsabile del trattamento.

La designazione del Responsabile viene effettuata mediante "accordo di nomina" sottoscritto da parte del Titolare del trattamento e controfirmato per accettazione da parte del Responsabile "esterno": il documento deve essere richiamato dagli accordi, convenzioni o contratti che prevedono l'affidamento di trattamenti di dati personali esternamente all'Azienda.

L'accettazione della nomina e l'impegno a rispettare le disposizioni del presente Regolamento è condizione necessaria per l'instaurarsi del rapporto giuridico fra le Parti.

## 25. Autorizzato al trattamento dei dati

Il Regolamento Europeo non fornisce rilievo autonomo alla figura dell' incaricato al trattamento dei dati, seppure si soffermi sul fatto che chi tratta dati, ricevendo istruzioni e formazione da parte del Titolare del trattamento debba da questi essere "autorizzato" al trattamento (articoli 4 e 10 del Regolamento).

Come già stabilito all'articolo 6 del presente Regolamento, al momento dell'ingresso in servizio è fornita, a cura dell'Ufficio Personale, ad ogni dipendente (oltre che ad ogni collaboratore o consulente a cura del competente Ufficio) una specifica comunicazione in materia di privacy, con apposita clausola inserita nel contratto di lavoro (o nella lettera di incarico per i summenzionati soggetti non dipendenti) , con la quale detti soggetti (dipendenti e non dipendenti) vengono nominati quali "autorizzati al trattamento dei dati" ai sensi del Regolamento UE 2016/679.

Contestualmente alla nomina dovrà essere data copia del presente Regolamento o, in alternativa, indicazioni per poterla scaricare dal sito internet aziendale o intranet.

Il Regolamento contiene infatti tutti i principi fondamentali della materia, esposti in maniera semplice, chiara e puntuale e il dipendente (o il non dipendente nei termini di cui si è detto sopra), nel sottoscrivere il contratto di lavoro (o la lettera di autorizzato), è reso edotto dell'esistenza dell'anzidetto Regolamento e delle modalità di consultazione del medesimo.

Analoghe considerazioni valgono per la figura dell' autorizzato "esterno" : tutti coloro che svolgono un'attività di trattamento dei dati nell'ambito di questo Ente, pur non essendo dipendenti e neppure titolari di incarichi conferiti dalla medesima Azienda (quali consulenze, collaborazioni), devono essere designati da parte del Titolare tramite una lettera (o una nota) di nomina come autorizzati.

Ci si riferisce, a titolo esemplificativo, al personale tirocinante o al personale volontario che opera temporaneamente all'interno dell'Azienda in virtù di un accordo o di una convenzione per lo svolgimento, appunto, di tirocini formativi piuttosto che di attività di volontariato a sostegno degli ospiti residenti in struttura.

Il personale di cui si parla è soggetto agli stessi obblighi cui sono sottoposti tutti gli autorizzati "interni", in modo da garantire il pieno rispetto della tutela della riservatezza dei dati.

Nel caso di Autorizzati "esterni", l'accesso ai dati deve essere limitato, con particolare rigore, ai soli dati personali la cui conoscenza sia strettamente necessaria per l'adempimento dei compiti assegnati e connessi all'espletamento dell'attività.

## 26. Responsabile della Protezione dei Dati / Data Protection Officer (RPD/DPO)

Il Regolamento Europeo impone la nomina del Data Protection Officer (DPO, in italiano: Responsabile della protezione dei dati o 'RDP'), nei termini di cui all'articolo 37, 38 e 39 del Regolamento medesimo.

Chi svolge la funzione di RPD deve presentare caratteristiche di indipendenza ed autorevolezza, oltre che competenze manageriali. Non deve, inoltre, essere in conflitto di interessi in quanto il GDPR vieta di nominare RDP anche chi, solo in astratto, possa potenzialmente trovarsi in conflitto di interessi.

Si tratta di una figura di alta professionalità, a metà tra il consulente ed il revisore e non dovrebbe ricoprire ruoli gestionali rispetto all'attività dell'azienda o ai fini istituzionali della Pubblica Amministrazione.

Anche la Carbosulcis provvede al conferimento dell'incarico di cui si tratta, tenendo conto delle prescrizioni sin qui descritte.

Ai sensi dell'articolo 39 del Regolamento UE, i suoi compiti sono:

- sorvegliare l'osservanza del Regolamento , valutando i rischi di ogni trattamento alla luce della natura, dell'ambito di applicazione e delle finalità;
- fornire consulenza e pareri al Titolare, ai Responsabili del trattamento dei dati e agli incaricati relativamente all'applicazione degli obblighi europei in materia;
- collaborare con il titolare, laddove necessario, nel condurre una valutazione di impatto sulla protezione dei dati (DPIA);
- informare e sensibilizzare il titolare o il responsabile del trattamento, nonché i dipendenti di questi ultimi, riguardo agli obblighi derivanti dal regolamento e da altre disposizioni in materia di protezione dei dati;
- cooperare con il Garante e fungere da punto di contatto per il Garante su ogni questione connessa al trattamento;
- supportare il titolare o il responsabile in ogni attività connessa al trattamento di dati personali, anche con riguardo alla tenuta di un registro delle attività di trattamento .

Ai sensi dell'articolo 37 del Regolamento UE, Egli deve:

- possedere un'adeguata conoscenza della normativa e delle prassi di gestione dei dati personali , anche in termini di misure tecniche e organizzative o di misure atte a garantire la sicurezza dei dati. Non sono richieste attestazioni formali o l'iscrizione ad appositi albi professionali, anche se la partecipazione a master e corsi di studio/professionali può rappresentare un utile strumento per valutare il possesso di un livello adeguato di conoscenze;
- adempiere alle sue funzioni in piena indipendenza e in assenza di conflitti di interesse. In linea di principio, ciò significa che il RPD non può essere un soggetto che ricopre ruoli gestionali e che decide sulle finalità o sugli strumenti del trattamento di dati personali;

- operare alle dipendenze del titolare oppure sulla base di un contratto di servizio (RPD esterno);
- disporre di risorse umane e finanziarie , messe a disposizione dal Titolare, per adempiere ai suoi scopi.

Il Regolamento UE prevede la pubblicazione on line del curriculum del RDP, nonché la pubblicazione sul sito istituzionale dell'Ente dei "dati di contatto" del RDP : dati che debbono essere inseriti anche nell'informativa aziendale sul trattamento dei dati, così che il RDP sia agevolmente contattabile dai cittadini-utenti ma anche dal Garante per la privacy.

Sia che il RDP sia interno che esterno, è necessario stipulare con il medesimo un contratto ad hoc. Nel caso in cui il RDP sia un "esterno" (persona o società) tutte le clausole, oltre che il compenso per l'incarico, dovranno essere inserite in un apposito contratto di servizi, ove siano anche previste le risorse necessarie a far funzionare l'ufficio del RDP.

# PARTE QUINTA: SICUREZZA DEI DATI PERSONALI - MISURE DI CARATTERE INFORMATICO E TECNOLOGICO

## 27. Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita (Privacy by Design e Privacy by Default)

L'articolo n. 25 del Regolamento Europeo n. 2016/679 introduce il criterio sintetizzato dall'espressione inglese "data protection by default and by design" , ossia dalla necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili al fine di soddisfare i requisiti del regolamento e tutelare i diritti degli interessati, tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati.

Tutto questo deve avvenire a monte, prima di procedere al trattamento dei dati vero e proprio ( "sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso", secondo quanto afferma l'art. 25, paragrafo 1 del Regolamento UE) e richiede, pertanto, un'analisi preventiva ed un impegno applicativo da parte del Titolare che deve sostanziarsi in una serie di attività specifiche e dimostrabili.

## 28. Registro delle attività di trattamento

Tutti i titolari e i responsabili di trattamento, eccettuati gli organismi con meno di 250 dipendenti ma solo se non effettuano trattamenti a rischio (si veda l'articolo 30, paragrafo 5 del Regolamento UE), devono tenere un Registro delle attività di trattamento i cui contenuti sono indicati all'articolo 30 del medesimo Regolamento.

Si tratta di uno strumento fondamentale non soltanto ai fini dell'eventuale supervisione da parte del Garante, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'azienda o di un soggetto pubblico, indispensabile per ogni valutazione e analisi del rischio.

Il Registro (in forma cartacea e/o elettronica) deve essere esibito su richiesta del Garante. La tenuta del registro dei trattamenti non costituisce un adempimento formale bensì parte integrante di un sistema tecnologico di corretta gestione dei dati personali.

## 29. Protezione e sicurezza dei dati personali

Le misure di sicurezza devono "garantire un livello di sicurezza adeguato al rischio " del trattamento (articolo 32, paragrafo 1 del Regolamento UE); in questo senso, la lista di cui al paragrafo 1 dell'art. 32 è una lista aperta e non esaustiva ("tra le altre, se del caso").

Per lo stesso motivo, secondo il Regolamento UE non potranno sussistere dopo il 25 maggio 2018 obblighi generalizzati di adozione di misure "minime" di sicurezza (ex art. 33 Codice) poiché tale valutazione sarà rimessa, caso per caso, al titolare e al responsabile in rapporto ai rischi specificamente individuati come da art. 32 del regolamento.

Si richiama l'attenzione anche sulla possibilità di utilizzare l'adesione a specifici codici di condotta o a schemi di certificazione per attestare l'adeguatezza delle misure di sicurezza adottate.

Il 05 Giugno 2019 il Garante della Privacy ha emanato il " Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del D.Lgs 10 agosto 2018 n.101 " contenente le indicazioni specifiche per alcune fattispecie di trattamenti.

## 30. Notifica di una violazione dei dati personali all'autorità di controllo (Data Breach)

A partire dal 25 maggio 2018, tutti i titolari dovranno notificare all'Autorità di controllo le violazioni di dati personali di cui vengano a conoscenza, entro 72 ore e comunque "senza ingiustificato ritardo", ma soltanto se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati (si veda considerando 85 del GDPR); questa procedura va sotto il nome di "Data Breach". Pertanto, la notifica all'Autorità dell'avvenuta violazione non è obbligatoria, essendo subordinata alla valutazione del rischio per gli interessati che spetta, ancora una volta, al Titolare.

Se la probabilità di tale rischio è elevata, si dovrà informare della violazione anche gli interessati, sempre "senza ingiustificato ritardo"; fanno eccezione le circostanze indicate al paragrafo 3 dell'articolo 34 del Regolamento UE. I contenuti della notifica all'Autorità e della comunicazione agli interessati sono indicati, in via non esclusiva, agli art. 33 e 34 del regolamento, nonché dalle " Linee Guida in materia di notifica delle violazioni di dati personali – WP250, definite in base alle previsioni del Regolamento UE 2016/679 " adottate dal Gruppo di Lavoro Art.29 il 03 ottobre 2017 (versione emendata e adottata il 6 febbraio 2018) e dal Provvedimento del Garante sulla notifica delle violazioni dei dati personali del 30 Luglio 2019.

Il Titolare del trattamento, sentito il Data Protection Officer, adotta quindi le misure necessarie a documentare eventuali violazioni, essendo peraltro tenuto a fornire tale documentazione, su richiesta, al Garante in caso di accertamenti.

## 31. Valutazione di Impatto sulla Protezione dei Dati (DPIA)

Le misure di sicurezza devono "garantire un livello di sicurezza adeguato al rischio " del trattamento (articolo 32, paragrafo 1 del GDPR); in questo senso, la lista di cui al paragrafo 1 dell'art. 32 è una lista aperta e non esaustiva ("tra le altre, se del caso"). Fondamentali fra tali attività correlate alla sicurezza sono quelle connesse al secondo criterio individuato nel GDPR rispetto alla gestione degli obblighi dei titolari, ossia il rischio inerente al trattamento.

Quest'ultimo è da intendersi come rischio di impatti negativi sulle libertà e i diritti degli interessati (si vedano considerando 75-77 del GDPR); tali impatti dovranno essere analizzati attraverso un apposito processo di valutazione (si vedano artt. 35-36 del GDPR) tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il titolare ritiene di dover adottare per mitigare tali rischi.

All'esito di questa valutazione di impatto il Titolare potrà decidere in autonomia se iniziare il trattamento (avendo adottato le misure idonee a mitigare sufficientemente il rischio) ovvero consultare l'autorità di controllo competente per ottenere indicazioni su come gestire il rischio residuale; l'Autorità non avrà il compito di "autorizzare" il trattamento, bensì di indicare le misure ulteriori eventualmente da implementare a cura del titolare e potrà, ove necessario, adottare tutte le misure correttive ai sensi dell'articolo 58: dall'ammonimento del titolare fino alla limitazione o al divieto di procedere al trattamento.

## 32. Trasferimento di dati personali all'estero

Si fa rinvio ai principi dettati dal Regolamento Europeo agli articoli 44 e seguenti, nonché alle indicazioni che fossero dettate, in materia, dal Legislatore nazionale e dal Garante per la protezione dei dati personali.

## 33. Disciplina aziendale sulla videosorveglianza

Si fa rinvio al Regolamento Aziendale sulla Videosorveglianza.

## 34. Disciplina aziendale sull'utilizzo dei mezzi informatici e telematici

Si fa rinvio all'allegato B del presente Regolamento.

# PARTE SESTA: ATTUAZIONE IN AMBITO AZIENDALE

## 35. ENTRATA IN VIGORE E PUBBLICITÀ

Il presente Regolamento entrerà in vigore dalla data di adozione con atto deliberativo del Consiglio di Amministrazione. Il Regolamento verrà pubblicato sul sito internet aziendale, nonché sull'Intranet aziendale.

## 36. Disposizione finale relativa agli 'allegati tecnici'

Il testo del presente Regolamento potrà essere aggiornato a seguito di eventuali modifiche che intervengano rispetto alla vigente normativa, sia nazionale che europea, in materia di protezione dei dati personali.

Quanto, invece, ai n. 4 Allegati tecnici al presente Regolamento, si stabilisce quanto segue: poiché si tratta di "strumenti di lavoro quotidiano", essi saranno inevitabilmente oggetto di continue, quanto rapide integrazioni, modifiche e revisioni, in virtù sia delle necessità aziendali che delle esigenze imposte da una realtà normativa ed organizzativa tuttora in rapidissima evoluzione.

Gli eventuali aggiornamenti ai documenti tecnici allegati verranno, pertanto, inseriti in tempo reale sul sito internet aziendale nell'apposita sezione dedicata alla "privacy", prescindendo dall'adozione di appositi atti deliberativi di modifica del presente Regolamento e dandone pubblicità, così da consentire una rapida consultazione on line dei medesimi ed un contenuto sempre aggiornato degli stessi.

# ALLEGATI AL PRESENTE REGOLAMENTO

A. REGOLE PER L'ADOZIONE DELLE MISURE DI SICUREZZA
B. DISCIPLINARE PER L'UTILIZZO DELLA RETE INFORMATICA
C. DISCIPLINARE PER L'AUTORIZZATO AL TRATTAMENTO
D. ISTRUZIONI OPERATIVE SULLE CORRETTE MODALITÀ DI UTILIZZO DEGLI STRUMENTI IN SMART WORKING

# A. REGOLE PER L'ADOZIONE DELLE MISURE DI SICUREZZA

La valutazione delle misure di sicurezza da adottare deve essere concepita nel contesto del rischio a cui è rivolta. Pertanto le misure di sicurezza vanno viste nel loro senso più ampio del termine partendo dal principio che l'art. 32 del Regolamento EU recita " Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio ".

Di seguito vengono riportate alcune regole (non esaustive) e principi di base per diverse misure di sicurezza che verranno implementate nel tempo.

| MISURE | REGOLE / PRINCIPI DA OSSERVARE |
|---|---|
| Presenza di un sistema di allarme | È importante che l'Ente si doti di impianto d'antifurto a tutela del patrimonio delle informazioni contenute al suo interno. |
| Custodia dei dati in armadi blindati e/o ignifughi | È importante che gli uffici che trattano dati c.d. sensibili e giudiziari possano disporre di queste strutture per archiviare in modo consono tali informazioni. |
| Sistemi UPS e Generatori di corrente che garantiscano la continuità elettrica | Fondamentale a tutela delle attività soprattutto per gli strumenti elettronici. Da adottare necessariamente per tutti i server e per quei pc locali che non archiviano le informazioni sul server. |
| Digitazione password all'accensione del PC | Tutti i PC devono avere la password all'accensione del terminale, questo non vale solo come regola ma viene considerata una misura base di sicurezza. |
| Manutenzione programmata degli strumenti | Come tutte le macchine che si rispettano anche il sistema informativo va manutenzionato periodicamente sia attraverso l'aggiornamento dei suoi componenti sia con la pulizia periodica delle macchine stesse. |
| Utilizzo di un sistema firewall | Obbligatorio viste le forme di attacco sempre più intelligenti. |
| Presenza di un sistema di autenticazione delle credenziali per tutti gli accessi agli archivi elettronici | Si intende con questa misura l'adozione di un server di dominio che consenta l'autenticazione dell'utente. |

| | |
|---|---|
| Disattivazione delle credenziali di autenticazione nel caso di inutilizzo per 6 mesi | Disattivare le credenziali che hanno perso efficacia |
| Controllo degli accessi a siti internet non sicuri – Protezione della posta elettronica | È importante la conoscenza da parte degli operatori della navigazione in internet e dell'uso della posta elettronica. |
| Utilizzo di un filtro anti-spam | All'interno dello spam (posta indesiderata) si annidano spesso dei fenomeni di illegalità informatica. È importante dotarsi di tale strumento |
| Utilizzo di un antivirus | Per quanto precedentemente detto, è importante la presenza di un antivirus in ogni posto di lavoro, considerata misura di sicurezza e ovviamente che sia aggiornato |
| Aggiornamento periodico di programmi per il controllo della vulnerabilità | È importante che ogni pc sia periodicamente aggiornato sulle proprie vulnerabilità con gli appositi software. |
| Disattivazione delle credenziali di autenticazione in caso di perdita di qualità dell'autorizzato | Disattivare le credenziali che hanno perso efficacia |
| Aggiornamento periodico, con cadenza almeno annuale, della lista dei profili di autorizzazione | Tutte le persone che operano all'interno degli uffici devono essere autorizzate dal Titolare |
| Istruzioni in merito alla segretezza e alla custodia delle credenziali di autenticazione | Rientra nel concetto della formazione del personale |
| Procedure di verifica sull'operato degli autorizzati | È un compito ispettivo dei Responsabili/Dirigenti |
| Formazione sugli aspetti principali della disciplina della privacy al momento dell'ingresso in servizio | Rientra nel concetto della formazione del personale |
| Formazione, periodica e in occasione di cambiamenti di mansioni o di introduzione di nuovi strumenti per il trattamento dei dati e la loro protezione | Rientra nel concetto della formazione del personale |
| Istruzioni finalizzate al controllo e alla custodia dei documenti contenenti dati personali per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento | Rientra nel concetto della formazione del personale |
| Adozione di procedure per le copie di sicurezza, la loro custodia ed il ripristino della disponibilità dei dati | Il backup deve essere metodico, non affidato alle singole volontà. |

| | |
|---|---|
| Definizioni di responsabilità e sanzioni disciplinari | Rientra nel concetto della formazione del personale nonché è necessario integrare il codice di comportamento includendo sanzioni disciplinari nei casi in cui ci sia un comportamento difforme da quando indicato dal presente Regolamento |
| Formazione professionale | Rientra nel concetto della formazione del personale |
| Distruzione del cartaceo | È importante nel limite del possibile incentivare la distruzione del cartaceo rendendolo illeggibile usando dei comodi distruggi documenti |
| Definizione di procedure per le copie di sicurezza, la loro custodia e il ripristino dei dati | Il salvataggio dei dati è fondamentale in qualsiasi organizzazione |
| I dati cartacei sono chiusi in un armadio | Ogni documento deve essere possibilmente chiuso in un armadio. Qualora questo non possa essere possibile, sicuramente che possano essere chiusi i dati sensibili e quelli giudiziari |

# B. DISCIPLINARE PER L'UTILIZZO DELLA RETE INFORMATICA

## 1. Oggetto e ambito di applicazione

Il presente regolamento si applica a tutte le "navigazioni" effettuate dagli utenti Interni ed Esterni che sono autorizzati ad accedere alla Rete dell'Azienda e tramite essa utilizzano delle risorse esterne alla struttura utilizzando il protocollo HTTP e HTTPS.

## 2. Principi generali – Diritti e Responsabilità

"L'utilizzo di Internet da parte dei lavoratori può infatti formare oggetto di analisi, profilazione e integrale ricostruzione mediante elaborazione di log file della navigazione web ottenuti, ad esempio, da un proxy server o da un altro strumento di registrazione delle informazioni. I servizi di posta elettronica sono parimenti suscettibili (anche attraverso la tenuta di log file di traffico e-mail e l'archiviazione di messaggi) di controlli che possono giungere fino alla conoscenza da parte del datore di lavoro (titolare del trattamento) del contenuto della corrispondenza".

## 3. Utilizzo dei Personal Computer.

Il Personal Computer affidato al dipendente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza e pertanto è vietato.

In particolare:

a. L'accesso all'elaboratore deve essere protetto da password che deve essere custodita dall'autorizzato con la massima diligenza e non divulgata. La password deve essere attivata per l'accesso alla rete, per lo screensaver e per il software applicativo;

b. L'Amministratore di Sistema, nell'espletamento delle sue funzioni legate alla sicurezza e alla manutenzione informatica, avrà la facoltà di accedere in qualunque momento anche da remoto (dopo aver richiesto l'autorizzazione all'utente interessato) al personal computer di ciascuno;

c. Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio. Lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. Deve essere attivato su tutti i Personal Computer lo screen saver e la relativa password;

d. L'accesso ai dati presenti nel personal computer potrà avvenire quando si rende indispensabile ed indifferibile l'intervento, ad esempio in caso di prolungata assenza od impedimento dell'autorizzato, informando lo stesso tempestivamente dell'intervento di accesso realizzato;

e. È vietato installare autonomamente programmi informatici salvo autorizzazione esplicita dell'Amministratore di Sistema, in quanto sussiste il grave pericolo di portare Virus informatici o di alterare la stabilità delle applicazioni dell'elaboratore. L'inosservanza di questa disposizione, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre la struttura a gravi responsabilità civili ed anche penali in caso di violazione della normativa a tutela dei diritti d'autore sul software che impone la presenza nel sistema di software regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore.

f. È vietato modificare le caratteristiche impostate sul proprio PC, salvo con autorizzazione esplicita dell'Amministratore di Sistema;

g. È vietato inserire password locali alle risorse informatiche assegnate (come ad esempio password che non rendano accessibile il computer agli amministratori di rete), se non espressamente autorizzati e dovutamente comunicate all'Amministratore di Sistema;

h. È vietata l'installazione sul proprio PC di dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, pendrive, dischi esterni, i-pod, telefoni, ecc.), se non con l'autorizzazione espressa dell'Amministratore di Sistema. Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente l'Amministratore di Sistema nel caso in cui vengano rilevati virus o eventuali malfunzionamenti.

**4. Utilizzo della rete informatica.**

Le unità di rete sono aree di condivisione di informazioni strettamente professionali sulle quali vengono svolte regolari attività di controllo, amministrazione e backup e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato in queste unità, nemmeno per brevi periodi.

Si parte quindi dal presupposto che i files relativi alla produttività individuale vengono salvati sul server e i limiti di accesso sono regolarizzati da apposite policies di sicurezza che suddividono gli accessi tra gruppi e utenti.

L'amministratore di Sistema può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza o in violazione del presente regolamento sia sui PC degli incaricati sia sulle unità di rete.

Le password d'ingresso alla rete ed ai programmi sono segrete e non vanno comunicate a terzi.

Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. È infatti assolutamente da evitare un'archiviazione ridondante.

E' importante togliere tutte le condivisioni dei dischi o di altri supporti configurate nel Personal Computer se non strettamente necessarie (e per breve tempo) allo scambio dei files con altri colleghi. Esse sono infatti un ottimo "aiuto" per i software che cercano di "minare" la sicurezza dell'intero sistema.

Sarà compito dell'Amministratore di Sistema provvedere alla creazione di un'area condivisa sul server per lo scambio dei dati tra i vari utenti.

Nell'utilizzo della rete informatica è fatto divieto di:

a. Utilizzare la Rete in modo difforme da quanto previsto dal presente regolamento;

b. Conseguire l'accesso non autorizzato a risorse di rete interne ed esterne alla Rete dell'Ente;

c. Agire deliberatamente con attività che influenzino negativamente la regolare operatività della Rete e ne restringano l'utilizzabilità e le prestazioni per altri utenti;

d. Effettuare trasferimenti non autorizzati di informazioni (software, dati, ecc);

e. Installare componenti hardware non compatibili con l'attività istituzionale;

f. Rimuovere, danneggiare o asportare componenti hardware;

g. Utilizzare qualunque tipo di sistema informatico o elettronico per controllare le attività di altri utenti, per leggere, copiare o cancellare files e software di altri utenti;

h. Usare l'anonimato o servirsi di risorse che consentano di restare anonimi;

**5. Utilizzo di internet**

I Personal Computer, qualora abilitati alla navigazione in Internet, costituiscono uno strumento necessario allo svolgimento della propria attività lavorativa.

Nell'uso di Internet e della Posta Elettronica non sono consentite le seguenti attività:

a. L'uso di Internet per motivi personali;

b. L'accesso a siti inappropriati (esempio siti pornografici, di intrattenimento, ecc.);

c. Lo scaricamento (download) di software e di file non necessari all'attività istituzionale;

d. Accedere a flussi in streaming audio/video da Internet per scopi non istituzionali (ad esempio ascoltare la radio o guardare video o filmati utilizzando le risorse Internet);

e. Un uso che possa in qualche modo recare qualsiasi danno all'Ente o a terzi;

**6. Utilizzo della posta elettronica**

La casella di posta, assegnata dall'Ente, è uno strumento di lavoro.

Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

È fatto divieto di utilizzare le caselle di posta elettronica della struttura per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mailing-list salvo diversa ed esplicita autorizzazione.

È buona norma evitare messaggi completamente estranei al rapporto di lavoro o alle relazioni tra colleghi. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali con l'Ente ricevuta da personale non autorizzato, deve essere visionata ed inoltrata al Responsabile d'Ufficio, o in ogni modo è opportuno fare riferimento alle procedure in essere per la corrispondenza ordinaria.

La documentazione elettronica che viene contraddistinta da diciture od avvertenze dirette ad evidenziarne il carattere riservato o segreto, non può essere comunicata all'esterno senza preventiva autorizzazione del Titolare del trattamento.

È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario.

Per la trasmissione di file all'interno della struttura è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati (ad esempio per dimensioni superiori a 2 Mbyte è preferibile utilizzare le cartelle di rete condivise).

È obbligatorio controllare i file Attachments di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web, HTTP o FTP non conosciuti) e accertarsi dell'identità del mittente.

Tutti coloro provvisti di indirizzo individuale, devono indicare il tutor del proprio account ossia la persona autorizzata ad aprire la posta del soggetto assente o quantomeno la persona che riceverà la posta del lavoratore assente.

Dopo sei mesi di assenza, l'account verrà disattivato e con esso la posta sarà trasferita ad un nuovo utente.

Per motivi di sicurezza la struttura non consente in alcun modo l'utilizzo di posta personale né attraverso l'uso di un webmail né utilizzando un client di posta.

In particolare nell'uso della Posta Elettronica non sono consentite le seguenti attività:

a. La trasmissione a mezzo di posta elettronica di dati sensibili, confidenziali e personali di alcun genere, salvo i casi espressamente previsti dalla normativa vigente in materia di protezione dei dati personali;

b. L'apertura di allegati ai messaggi di posta elettronica senza il previo accertamento dell'identità del mittente;

c. Inviare tramite posta elettronica user-id, password, configurazioni della rete interna, indirizzi e nomi dei sistemi informatici;

d. Inoltrare "catene" di posta elettronica (catene di S.Antonio e simili), anche se afferenti a presunti problemi di sicurezza.

**7. Utilizzo delle password**

Le password di ingresso alla rete, di accesso ai programmi e dello screen saver, sono previste ed attribuite all'Autorizzato.

È necessario procedere alla modifica della password al primo utilizzo e, successivamente, almeno ogni tre/sei mesi.

Le password possono essere formate da lettere (maiuscole o minuscole), numeri e caratteri speciali, ricordando che lettere maiuscole e minuscole hanno significati diversi per il sistema; devono essere composte da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'autorizzato.

La password deve essere immediatamente sostituita nel caso si sospetti che la stessa abbia perso la segretezza.

Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia, per iscritto, all'Amministratore di Sistema dell'Ente.

**8. Utilizzo dei supporti magnetici**

Tutti i supporti magnetici riutilizzabili (dischetti, nastri, DAT, chiavi USB, CD riscrivibili) contenenti dati sensibili e giudiziari devono essere trattati con particolare cautela onde evitare che il loro

contenuto possa essere recuperato. Una persona esperta potrebbe infatti recuperare i dati memorizzati anche dopo la loro cancellazione.

I supporti magnetici contenenti dati sensibili e giudiziari devono essere custoditi in archivi chiusi a chiave.

Tutti i supporti magnetici riutilizzabili (dischetti, nastri, DAT, chiavi USB, CD riscrivibili) obsoleti devono essere consegnati all'Amministratore di Sistema per l'opportuna distruzione.

Ogni qualvolta si procederà alla dismissione di un Personal Computer l'Amministratore di Sistema provvederà alla distruzione delle unità di memoria interne alla macchina stessa (hard- disk, memorie allo stato solido).

**9. Utilizzo di pc portatili**

L'utente è responsabile del PC portatile assegnatogli e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

Ai PC portatili si applicano le regole di utilizzo previste per i PC connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.

I PC portatili utilizzati all'esterno (convegni, seminari, ecc…), in caso di allontanamento devono essere custoditi in un luogo protetto.

**10. Utilizzo delle stampanti e dei materiali di consumo**

L'utilizzo delle stampanti e dei materiali di consumo in genere (carta, inchiostro, toner, floppy disk, supporti digitali come CD e DVD) è riservato esclusivamente ai compiti di natura strettamente istituzionale.

Devono essere evitati in ogni modo sprechi dei suddetti materiali o utilizzi eccessivi.

È cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni. È buona regola evitare di stampare documenti o file non adatti (molto lunghi o non supportati, come ad esempio il formato pdf o file di contenuto grafico) su stampanti comuni. In caso di necessità la stampa in corso può essere cancellata.

**11. Osservanza delle disposizioni in materia di Privacy**

È obbligatorio attenersi alle disposizioni in materia di Privacy e di misure di sicurezza.

**12. Amministrazione delle risorse informatiche**

L'Amministratore di Sistema è il soggetto cui è conferito il compito di sovrintendere alle Risorse Informatiche dell'Ente e a cui sono consentite in maniera esclusiva le seguenti attività:

a. Gestire l'hardware e il software di tutte le strutture tecniche informatiche di appartenenza dell'Ente collegate in rete o meno;

b. Gestire esecutivamente (creazione, attivazione, disattivazione e tutte le relative attività amministrative) gli account di rete e i relativi privilegi di accesso alle risorse, assegnati agli utenti della Rete Informatica dell'Ente;

c. Monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare il corretto utilizzo delle risorse di rete, dei computer e degli applicativi, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori;

d. Creare, modificare, rimuovere o utilizzare qualunque account o privilegio, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori;

e. Rimuovere programmi software dalle risorse informatiche assegnate agli utenti, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori;

f. Rimuovere componenti hardware dalle risorse informatiche assegnate agli utenti, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori;

g. Utilizzare le credenziali di accesso di amministrazione del sistema, o l'account di un utente tramite reinizializzazione della relativa password, per accedere ai dati o alle applicazioni presenti su una risorsa informatica assegnata ad un utente in caso di prolungata assenza, irrintracciabilità o impedimento dello stesso. Tale utilizzo deve essere esplicitamente richiesto dal Responsabile dell'utente assente o impedito e deve essere limitato al tempo strettamente necessario al compimento delle attività indifferibili per cui è stato richiesto.

## 13. Non osservanza del Regolamento

Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite.

La contravvenzione alle regole contenute nel presente regolamento da parte di un utente, comporta l'immediata revoca delle autorizzazioni ad accedere alla Rete Informatica ed ai servizi/programmi autorizzati, fatte salve le sanzioni più gravi previste dalle norme vigenti.

Se i lavoratori perseverassero nell'uso ed abuso degli strumenti elettronici a loro disposizione, il datore è autorizzato a procedere per step, con controlli prima sul reparto, poi sull'ufficio e, infine, sul gruppo di lavoro; solo a questo punto, ripetendosi l'anomalia, sarà lecito il controllo su base individuale.

## 14. Aggiornamento e revisione

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento. Le proposte verranno esaminate dall'Ente.

Il presente Regolamento è soggetto a revisione.

# C. DISCIPLINARE PER L'AUTORIZZATO AL TRATTAMENTO

Per i trattamenti di dati personali effettuato con l'ausilio di strumenti elettronici, gli Autorizzati al trattamento dei dati personali debbono osservare le seguenti disposizioni.

Gli stessi sono autorizzati ad effettuare esclusivamente i trattamenti di dati che rientrano nell'ambito di trattamento definito e comunicato all'atto della designazione, con la conseguente possibilità di accesso ed utilizzo della documentazione cartacea e degli strumenti informatici, elettronici e telematici e delle banche dati aziendali che contengono i predetti dati personali.

Il trattamento dei dati personali deve essere effettuato esclusivamente in conformità alle finalità previste e dichiarate e, pertanto, in conformità alle informazioni comunicate agli interessati.

L'Autorizzato al trattamento dei dati personali deve prestare particolare attenzione all'esattezza dei dati trattati e, se sono inesatti o incompleti, deve provvedere ad aggiornarli tempestivamente

Ogni Autorizzato al trattamento dei dati personali è tenuto ad osservare tutte le misure di protezione e sicurezza atte a evitare rischi di distruzione o perdita anche accidentale dei dati, accesso non autorizzato, trattamento non consentito o non conforme alle finalità della raccolta.

Gli Autorizzati al trattamento dei dati personali che hanno ricevuto le credenziali di autenticazione per il trattamento dei dati personali, debbono conservare con la massima segretezza le componenti riservate delle credenziali di autenticazione (parole chiave) e i dispositivi di autenticazione in loro possesso e uso esclusivo.

La parola chiave, quando è prevista dal sistema di autenticazione, deve essere composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito.

La componente riservata delle credenziali di autenticazione (parola chiave) non deve contenere riferimenti agevolmente riconducibili all'Autorizzato.

L'Autorizzato del trattamento dei dati personali deve modificare la componente riservata delle credenziali di autenticazione (parola chiave) al primo utilizzo e, successivamente, almeno ogni tre/sei mesi.

In caso di trattamento di dati sensibili e di dati giudiziari la componente riservata delle credenziali di autenticazione (parola chiave) deve essere modificata almeno ogni tre mesi.

Gli autorizzati al trattamento non debbono in nessun caso lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento dei dati personali.

Per i trattamenti di dati personali effettuato senza l'ausilio di strumenti elettronici gli autorizzati al trattamento dei dati personali debbono osservare le seguenti disposizioni:

- I documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici non devono essere portati al di fuori dei locali individuati per la loro conservazione se non in casi del tutto eccezionali, e nel caso questo avvenga, l'asportazione deve essere ridotta al tempo minimo necessario per effettuare le operazioni di trattamento.

- Per tutto il periodo in cui i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici sono al di fuori dei locali individuati per la loro conservazione, l'Autorizzato del trattamento non dovrà lasciarli mai incustoditi.
- L'Autorizzato del trattamento deve inoltre controllare che i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici, composti da numerose pagine o più raccoglitori, siano sempre completi e integri.
- Al termine dell'orario di lavoro l'Autorizzato del trattamento deve riportare tutti i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici, nei locali individuati per la loro conservazione.
- I documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici non devono essere mai lasciati incustoditi sul tavolo durante l'orario di lavoro.
- Si deve adottare ogni cautela affinchè ogni persona non autorizzata, possa venire a conoscenza del contenuto di documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici.
- Per evitare il rischio di diffusione dei dati personali trattati senza l'ausilio di strumenti elettronici, si deve limitare l'utilizzo di copie fotostatiche.
- Particolare cautela deve essere adottata quando i documenti sono consegnati in originale a un altro Autorizzato debitamente autorizzato.
- Documenti contenenti dati personali sensibili o dati che, per una qualunque ragione siano stati indicati come meritevoli di particolare attenzione, devono essere custoditi con molta cura.
- E' inoltre tassativamente proibito utilizzare copie fotostatiche di documenti (anche se non perfettamente riuscite) all'esterno del posto di lavoro, né tantomeno si possono utilizzare come carta per appunti.
- Documenti contenenti dati personali che, per una qualunque ragione, siano da cestinare, devono assolutamente essere distrutti in modo da risultare illeggibili a soggetti terzi non autorizzati che ne potrebbero entrare in possesso (es. addetti alle pulizie).
- Quando i documenti devono essere trasportati essere portati al di fuori dei locali individuati per la loro conservazione o addirittura all'esterno del luogo di lavoro, l'Autorizzato del trattamento deve tenere sempre con sé la cartella o la borsa, nella quale i documenti sono contenuti.
- L'Autorizzato del trattamento deve inoltre evitare che un soggetto terzo non autorizzato al trattamento possa esaminare, anche solo la copertina del documento in questione.
- E' proibito discutere, comunicare o comunque trattare dati personali per telefono, se non si è certi che il destinatario sia un autorizzato a potere trattare i dati in questione.
- Si raccomanda vivamente di non parlare mai ad alta voce, trattando dati personali per telefono, soprattutto utilizzando apparati cellulari, in presenza di terzi non autorizzati, per evitare che i dati personali possano essere conosciuti da terzi non autorizzati, anche accidentalmente. Queste precauzioni diventano particolarmente importanti, quando il telefono è utilizzato in luogo pubblico o aperto al pubblico.

# D. ISTRUZIONI OPERATIVE SULLE CORRETTE MODALITÀ DI UTILIZZO DEGLI STRUMENTI IN SMART WORKING

## 1. Premesse e applicazione

Con il presente regolamento la Carbosulcis spa intende disciplinare le norme comportamentali che tutto il personale in servizio cui è stato comunicato di operare in smart working deve rispettare.

Per quanto non previsto in questo documento, si richiamano comunque nel loro complesso le norme di legge, compreso quanto previsto dal contratto collettivo nazionale di lavoro riguardanti i doveri dei lavoratori.

Le presenti Istruzioni hanno come scopo quello di indicare le misure organizzative aventi l'obiettivo di proteggere tutti i dati trattati dall'azienda.

Divieto di comunicazione e divulgazione

È fatto assoluto divieto di comunicazione e divulgazione di qualsivoglia dato che l'incaricato è autorizzato a trattare, se non previa autorizzazione del proprio responsabile il quale, in caso di dubbio o di situazioni particolarmente delicate, può rivolgersi direttamente al datore di lavoro, che darà eventuale autorizzazione. Tale divieto si intende esteso anche al periodo successivo alla scadenza dell'incarico o del rapporto di lavoro e comunque sino a quando le suddette informazioni non vengano divulgate ad opera del datore di lavoro oppure divengano di dominio pubblico.

## 2. Istruzioni per il corretto trattamento dati con strumenti informatici con strumenti forniti dall'Azienda

Utilizzo degli strumenti aziendali

Come è noto, gli strumenti di lavoro sono sotto la responsabilità dell'azienda stessa, che li mette a disposizione (eventualmente) dei propri addetti alle seguenti condizioni:

- gli strumenti possono essere utilizzati solo per fini professionali (in relazione alle mansioni assegnate);
- gli strumenti vengono custoditi con cura dal lavoratore cui sono assegnati, evitando manomissioni, danneggiamenti o utilizzi, anche da parte di altre persone, per scopi non consentiti;
- vengono sempre rispettate le presenti istruzioni e le norme di buon comportamento.

Utilizzo di telefono mobile

In sede di eventuale consegna di un telefono cellulare, palmare, blackberry, smartphone, tablet o simili, il datore di lavoro ne disciplina l'uso per finalità diversa dall'esecuzione delle prestazioni lavorative.

Si precisa comunque che il dispositivo è e resta di proprietà dell'azienda, che ha facoltà di esercitare in qualsiasi momento ogni diritto previsto dalle disposizioni legislative vigenti.

I dipendenti e i collaboratori sono responsabili della corretta custodia del bene e durante l'utilizzazione dello stesso dovranno comportarsi in maniera diligente e responsabile, garantendo l'integrità materiale e del suo impiego.

In caso di danneggiamento, furto, smarrimento o utilizzo illecito, potranno essere attivate azioni di natura disciplinare e afferenti il risarcimento del danno come previsto dagli artt. 1218, 2043 e ss. cod. civ.

Si precisa inoltre che:

- il gestore telefonico fornisce i tabulati delle telefonate effettuate da ciascuna utenza dell'Azienda e che pertanto quest'ultima potrà, in caso di necessità, effettuare controlli sul corretto utilizzo;
- i dati salvati sul telefono (rubrica, agenda) sono e restano di esclusiva responsabilità del singolo utente, che deve occuparsi di provvedere ai necessari back – up o salvataggi;
- qualsiasi problema, disfunzione o rottura del telefono, va comunicata all'Ufficio di riferimento;
- in caso di interruzione del rapporto di lavoro tutti i dati aziendali presenti nel telefono (es. rubrica telefonica) devono essere restituiti unitamente all'apparecchio.

Utilizzo dei computer

Ad ogni utilizzo di un PC o di computer fisso, l'addetto si assume la responsabilità del corretto utilizzo dello strumento nel rispetto delle istruzioni che seguono:

- le postazioni sono configurate secondo gli standard Aziendali e qualsiasi modifica deve essere autorizzata dall'Amministratore di sistema, responsabile dei servizi informativi;
- è vietata l'istallazione sul computer di qualsiasi tipo di software senza l'autorizzazione della Direzione, al fine di prevenire l'istallazione di software pericolosi (quali ad esempio virus informatici che possono alterare la stabilità dei sistemi operativi) o sprovvisti di regolare licenza d'uso;
- è vietato, se non a seguito di esplicito consenso o richiesta da parte dell'azienda, collegare il computer ad altri computer, reti esterne, a modem, a router, a schede di rete o a qualsiasi dispositivo compreso telefono cellulare o periferica che non siano quelle previste dall'Azienda;
- in presenza di terzi, è necessario accertarsi che questi non possano leggere le informazioni sul PC;
- è fatto divieto di caricare sul PC dati estranei all'attività lavorativa;
- una volta attivato il PC, è opportuno non lasciare incustodita la postazione senza prima averne bloccato l'accesso;
- l'utilizzo di eventuali supporti esterni - oltre a dover essere autorizzato - deve essere preceduto da una opportuna verifica che accerti: l'origine del supporto, il suo contenuto e l'assenza di virus al suo interno;
- non è consentito utilizzare programmi informatici o strumenti per intercettare, falsificare, alterare o sopprimere per finalità illecite il contenuto di comunicazioni e/o documenti informatici.

L'azienda si riserva la facoltà di procedere alla rimozione di ogni file o applicazione che riterrà essere potenzialmente pericolosi per la sicurezza del sistema, ovvero acquisiti o istallati in violazione del presente regolamento.

**3. Istruzioni per il corretto trattamento dati con strumenti informatici con strumenti personali**

Dotazioni degli strumenti

Qualora il dipendente utilizzi propri device, gli strumenti devono essere dotati almeno delle seguenti misure minime

- Software aggiornato
- Antivirus
- Accesso ad uno spazio cloud per effettuare il backup dei dati

Password

È obbligatorio l'uso corretto della propria password di accesso al PC, del cui utilizzo ogni autorizzato è pienamente responsabile. È indispensabile che ciascun autorizzato prenda nota delle buone modalità con cui è possibile selezionare parole chiave di difficile individuazione, seguendo le norme indicate di seguito. Qualora si abbia il sospetto che la propria password sia stata in qualche modo compromessa o venuta a conoscenza di terzi, si raccomanda di provvedere immediatamente alla sua sostituzione e riferire l'accaduto al responsabile aziendale.

Ai fini di mantenere l'adeguata protezione della propria password:

- la parola chiave prescelta non deve mai contenere riferimenti personali (nomi, date di nascita, ecc...), né dovrebbe rappresentare una parola in qualsiasi lingua o dialetto sufficientemente diffuso;
- si suggerisce di selezionare una nomenclatura della password adeguatamente lunga (minimo 8 caratteri) e complessa (caratteri minuscoli, maiuscoli e un caratteri speciali);
- si raccomanda di non utilizzare la stessa password utilizzata in altri sistemi di autenticazione, interni o esterni all'azienda, come ad esempio l'accesso al proprio conto corrente bancario e/o altre attività non legate all'attività aziendale;
- non è permesso condividere o concedere l'uso della parola chiave prescelta con alcun soggetto, interno o esterno all'azienda;
- al momento in cui si sostituisce la propria password, la nuova selezionata dovrebbe essere diversa da quelle già utilizzate in precedenza.

Posta elettronica

La posta elettronica diretta all'esterno della rete informatica aziendale può essere intercettata da estranei, ed è pertanto sconsigliato l'invio di documenti di lavoro riservati senza l'utilizzo di adeguate protezioni.

L'invio di documenti o dati mediante posta elettronica deve sempre essere effettuato con le dovute cautele, quali accertarsi che il destinatario sia autorizzato a trattare i dati inviati, che l'indirizzo sia corretto, che il destinatario riceva correttamente i documenti inviati (ad es. mediante conferma di lettura), ecc.

Per eventuali necessità, si suggerisce di apporre il seguente testo standard in calce:

"Le informazioni contenute in questo messaggio, sono riservate e ad uso esclusivo del destinatario. La diffusione, distribuzione e/o la copiatura del documento trasmesso da parte di qualsiasi soggetto diverso dal destinatario è proibita, sia ai sensi dell'art. 616 c.p., e ai sensi del D.Lgs. 196/2003 e ss.mm.ii. (D.Lgs. 101/2018) e del Regolamento Europeo 679/2016 (GDPR).

Nell'eventualità che questo messaggio Le fosse pervenuto per errore, La invitiamo ad eliminarlo senza copiarlo e a non inoltrarlo a terzi, dandocene gentilmente comunicazione. Grazie."

Protezione dei dati personali

La informiamo che il suo indirizzo è stato incluso nella banca dati della Carbosulcis spa, e viene utilizzato per fini istituzionali. Attraverso il seguente link (https://www.carbosulcis.eu/) è possibile prendere visione dell'informativa resa dal nostro sito, la stessa contiene i dati di contatto del Titolare del trattamento e del Responsabile della Protezione dei Dati (RPD/DPO), nonché le modalità attraverso il quale vengono trattati i Suoi dati e le altre informazioni utili.

 Rispetta il tuo ambiente: pensa prima di stampare questa mail

L'invio dei documenti contenenti dati particolari o particolarmente sensibili con la posta elettronica va effettuato previa protezione del documento con una password. Quest'ultima dovrà essere condivisa con il destinatario prima dell'invio o comunque con un mezzo separato rispetto all'email, nel cui corpo NON dovrà essere segnata in chiaro la password prescelta.

In generale, nell'utilizzo della posta elettronica come strumento di lavoro e di comunicazione tra i dipendenti, e tra questi e i terzi, si raccomanda in particolare di rispettare i criteri minimi di utilizzo riportati di seguito.

NON è consentito:

- dar luogo o rispondere a email "tipo catena di Sant'Antonio" dall'indirizzo aziendale;
- inviare immagini, file, video o scherzi elettronici dall'indirizzo aziendale;
- aprire allegati non sicuri, o inviati da fonti sconosciute;
- cancellare, anche parzialmente, le e-mail aziendali inviate e/o ricevute, salvo diversa autorizzazione;
- cancellare, anche parzialmente, la rubrica aziendale;
- cliccare su link.

***È invece obbligatorio***:

- eliminare tempestivamente messaggi "spam" o similari (onde evitare la diffusione di virus informatici).

Procedura d'emergenza

Qualora il Titolare necessiti di dover accedere al PC assegnato ad un dipendente ovvero alla Sua posta elettronica sarà onere del Responsabile di riferimento o della Direzione stabilirne le modalità che potranno essere diversificate area per area nel rispetto delle regole che seguono:

- il responsabile di riferimento d'accordo con il dipendente potrà individuare i colleghi autorizzati ad accedere alla sua casella di posta elettronica e/o alla propria postazione di lavoro in caso di assenza programmata;
- in caso di assenza non programmata, il dipendente potrà autorizzare anche telefonicamente il proprio responsabile o i propri colleghi ad accedere alla propria casella email e/o postazione di lavoro;
- in casi di necessità/urgenza/impossibilità a contattare il dipendente assente, l'Amministratore di Sistema, su richiesta della Direzione, potrà provvedere a resettare la password dell'utente per consentirne l'accesso. Tale operazione verrà comunicata al dipendente non appena possibile. Al suo rientro, questi imposterà una nuova password;
- in ogni caso, è fatto divieto di "rispondere" utilizzando l'account email del dipendente assente;
- ogni utente ha l'obbligo di inserire un messaggio automatico di assenza;
- qualora la parola chiave venga utilizzata in assenza dell'autorizzato, a quest'ultimo non compete più alcuna ulteriore responsabilità, in merito a trattamenti non autorizzati o accessi non consentiti ai dati. La sua responsabilità verrà pienamente rimessa in essere non appena avrà avuto la possibilità di selezionare una nuova parola chiave e assumere quindi la piena responsabilità del corretto utilizzo.

**4. Istruzioni per il corretto trattamento dati con strumenti cartacei**

Consegna dei documenti via posta

Nel caso la consegna di documenti, originali o fotocopiati contenenti dati particolari o informazioni qualificate come riservate, avvenga per posta, si richiede l'utilizzo di tipi di spedizione che garantiscano di tracciare i movimenti del documento (ad es. raccomandata A/R, etc.).

Quale che sia il tipo di spedizione adottato, si raccomanda di accertare che esso consenta di avere prova certa del fatto che il destinatario abbia effettivamente ricevuto i documenti inviati e che essi siano giunti integri, e quindi non manomessi o alterati in fase di trasporto.

Custodia dei documenti all'esterno dei luoghi di lavoro

Qualora per motivi di lavoro vengano trasportati documenti all'esterno del luogo di lavoro, l'incaricato deve tenere sempre sotto controllo il plico, avendo cura altresì che nessun soggetto terzo non autorizzato possa vedere anche solo la copertina del documento in questione.

**5. Conversazioni e comunicazioni telefoniche**

Si raccomanda di non discutere, comunicare o comunque trattare dati aziendali se non si è certi che il corrispondente sia un autorizzato a trattare i dati in questione.

Si raccomanda la massima attenzione nella scelta dei luoghi ove svolgere le conversazioni telefoniche.

**6. Social Network**

La divulgazione di informazioni all'esterno dovrà avvenire nel rispetto del principio di segretezza e riservatezza, nel rispetto del proprio profilo di autorizzazione e sempre salvaguardando l'immagine aziendale dell'azienda.