PREMESSA

A seguito dell'entrata in vigore del Regolamento UE 679/16 recante disposizioni in materia di protezione dei dati personali Cooperativa Dharma Soc.Coop , nel conformarsi alle novità introdotte, ha adottato la presente Policy aziendale al fine di individuare le norme comportamentali e le procedure tecnico-organizzative cui è necessario attenersi in materia di trattamento di dati personali e di sicurezza nello svolgimento di tutte le attività aziendali.

In particolare, Cooperativa Dharma Soc. Coop srl ritiene necessario definire una chiara disciplina interna atta a garantire che il trattamento dei dati personali svolto nell'ambito delle mansioni lavorative, avvenga nel rispetto dei diritti e delle libertà fondamentali dell'interessato con piena applicazione dei principi di riservatezza, liceità e correttezza.

AMBITO DI APPLICAZIONE DEL REGOLAMENTO

AMBITO SOGGETTIVO

Tutte le persone fisiche e giuridiche che, nell'esercizio delle proprie mansioni/attività/incarichi ed a qualsiasi titolo trattino per conto di Cooperativa Dharma Soc. Coop srl dati personali e sensibili sono tenuti al rispetto delle regole di seguito elencate.

AMBITO OGGETTIVO

Il regolamento si applica a tutti i trattamenti di dati personali di cui sia titolare COOPERATIVA DHARMA SOC.COOP (quali, ad es. attività connesse alla gestione del personale, agli adempimenti relativi ai propri clienti, fornitori ed eventuali consulenti, per cui la Società ha titolarità autonoma) ovvero a quelle attività che comportino da parte di Cooperativa Dharma Soc. Coop il trattamento di dati personali in qualità di Responsabile del Trattamento a seguito di apposita nomina nell'ambito delle istruzioni impartite di volta in volta dai Committenti e comunque sempre nel rispetto della normativa vigente in materia.

INFORMATIVE SUL TRATTAMENTO DEI DATI PERSONALI rilasciate da COOPERATIVA DHARMA SOC. COOP ai sensi dell'art. 13 del Reg. UE (GDPR)

Dati di titolarità di COOPERATIVA DHARMA SOC. COOP

Il trattamento dei dati personali e sensibili viene effettuato da Cooperativa Dharma Soc. Coop srl nel rispetto delle finalità e con le modalità indicate nell'informativa ai sensi dell'art. 13 del GDPR preliminarmente rilasciata agli interessati.

L'informativa al personale dipendente viene rilasciata, ed il relativo consenso acquisito, al momento della consegna della lettera di assunzione o a seguito di modifiche normative; l'informativa aggiornata viene altresì pubblicata sul sito internet aziendale www.dharmacoop.it.

L'informativa viene consegnata anche a Clienti e Fornitori al momento dell'inizio del rapporto.

VIOLAZIONE DEL REGOLAMENTO

Fermi restando i profili di responsabilità civile e penale, il trattamento illecito dei dati o la violazione delle misure di sicurezza approntate dall'azienda, costituisce un comportamento sanzionabile disciplinarmente in quanto grave violazione degli obblighi contrattualmente assunti, con conseguente applicabilità di sanzioni disciplinari ai sensi del vigente C.C.N.L. applicabile al rapporto di lavoro.

RINVIO

Per quanto non espressamente disciplinato in questa sede, si rinvia ai principi ed alle disposizioni del Regolamento UE 679/16 che qui deve intendersi integralmente richiamato.

DEFINIZIONI

Ai fini del presente Regolamento, si riportano di seguito le definizioni di maggiore rilevanza rispetto all'attività aziendale:

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

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

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

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

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

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

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

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

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

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

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

n) "posta elettronica", messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza.

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

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

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

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

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

ORGANIGRAMMA PRIVACY

TITOLARE DEL TRATTAMENTO

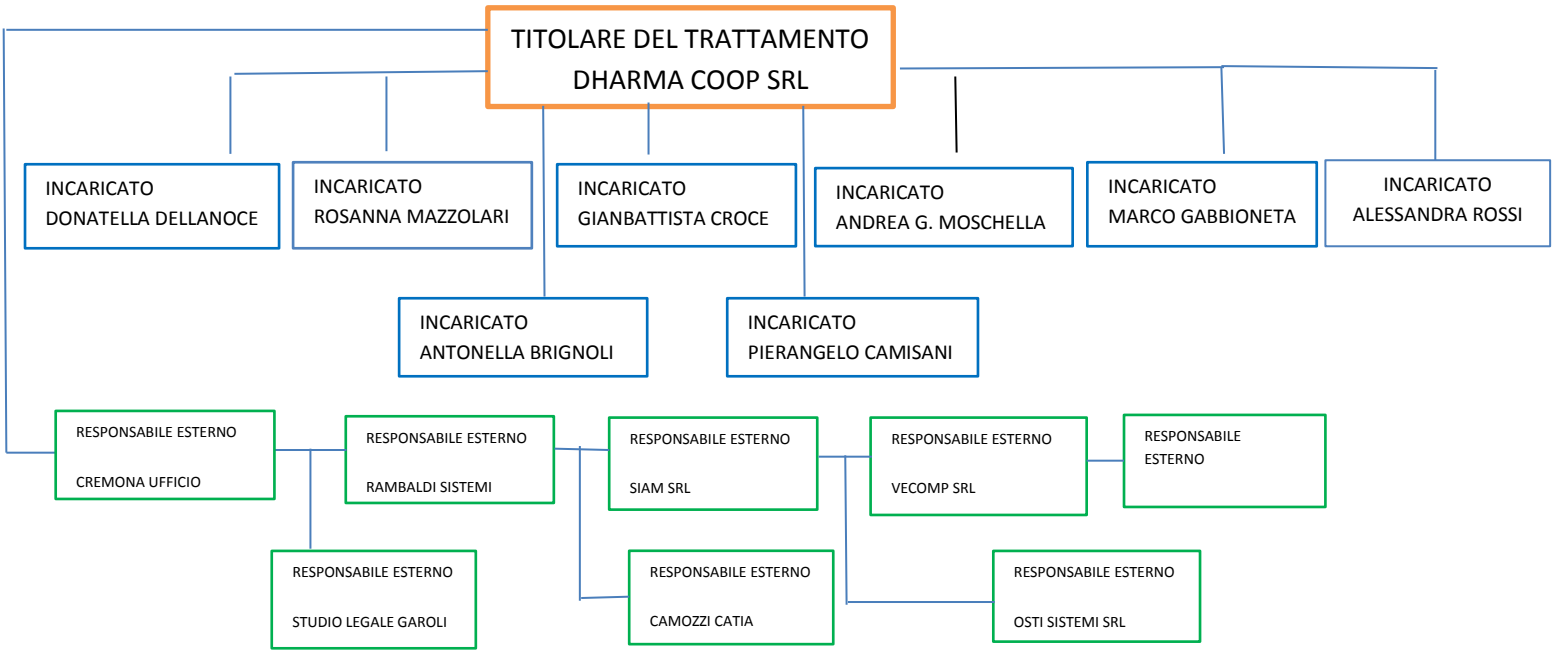
Il Titolare del trattamento è l'Ente nel suo complesso, rappresentato dall'Amministratore Delegato pro-tempore, in qualità di Legale Rappresentante.

RESPONSABILI ESTERNI

I soggetti esterni che, in qualità di fornitori, consulenti o comunque contraenti, per esigenze organizzative della Società, gestiscono specifici servizi o svolgono attività connesse, strumentali o di supporto a quelle della Società, e che pertanto effettuano attività di trattamento di dati personali di titolarità aziendale (ad es.: fornitura di prestazioni professionali o di prestazioni e servizi anche in convenzione quali consulenti, istituti di credito ed assicurativi, ecc.), sono di norma individuati in qualità di Responsabili del trattamento, sempreché in possesso dei requisiti previsti dal GDPR (esperienza, capacità, affidabilità).

INCARICATI DEL TRATTAMENTO

Gli Incaricati del trattamento sono i soggetti - nominati dal Titolare e/o dal Responsabile del trattamento - che trattano i dati personali cui hanno accesso nello svolgimento delle proprie funzioni attenendosi alle istruzioni loro impartite dal Titolare e/o dal Responsabile. Le risorse impiegate in mansioni che comportino trattamento di dati personali devono essere appositamente preposte con comunicazione scritta.



REGOLE OPERATIVE

REGOLE GENERALI PER TUTTI I TRATTAMENTI

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

2. i dati trattati devono essere aggiornati, corretti, pertinenti e completi.

3. i dati devono essere conservati per un tempo strettamente necessario al raggiungimento delle finalità per cui sono stati raccolti.

4. Ciascun incaricato è dotato di credenziali di autenticazione (userid + password) riservate e personali che consentono di accedere ai dati personali che è autorizzato a trattare, nonché ad utilizzare gli strumenti aziendali necessari per il trattamento. Le credenziali vengono disattivate al momento della cessazione del rapporto di lavoro.

5. Ciascun soggetto preposto allo svolgimento delle operazioni di trattamento ha l'obbligo di mantenere il segreto sui dati raccolti o di cui venga a conoscenza nel corso della propria attività lavorativa, evitando di diffonderli o di comunicarli a terzi senza previa autorizzazione della Società.

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

7. Qualora l'incaricato utilizzi, nello svolgimento delle proprie mansioni, atti/documenti contenenti dati personali o sensibili, questi non devono essere lasciati incustoditi ma occorre siano evitati eventuali accessi

o la conoscenza da parte di soggetti non autorizzati; alla fine del ciclo di lavoro, la documentazione deve essere SEMPRE riposta negli archivi ad accesso controllato;

8. Al momento della registrazione dei dati raccolti, occorre prestare attenzione alla digitazione e all'inserimento dei dati identificativi e degli altri dati riferiti all'interessato, al fine di evitare errori, che potrebbero generare problemi nella corretta gestione delle anagrafiche e nello svolgimento delle operazioni, che caratterizzano il processo di trattamento;

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

MISURE DI SICUREZZA

MISURE PER TRATTAMENTI EFFETTUATI CON STRUMENTI ELETTRONICI/INFORMATICI

Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati autorizzati dotati di credenziali di autenticazione che non devono essere condivise, cedute a terzi, lasciate incustodite, divulgate, contenere riferimenti facilmente riconducibili all'incaricato, memorizzate in processi di connessione automatica.

Gestione degli strumenti elettronici in dotazione

Ciascun incaricato è responsabile del corretto utilizzo e della custodia degli strumenti elettronici in dotazione (a titolo esemplificativo personal computer, periferiche, lettori di smart card, ecc.). Devono essere adottate le misure di sicurezza per la tutela della riservatezza, consistenti nell'evitare che l'accesso ai dati possa avvenire da parte di soggetti estranei all'organizzazione o non specificamente autorizzati.

Per monitorare il rispetto delle politiche e degli obblighi di sicurezza possono essere svolti controlli e ispezioni.

Nel caso di rilevato uso illecito o non autorizzato degli strumenti elettronici, ciò può costituire condotta disciplinarmente rilevante sanzionabile a norma del CCNL applicato al rapporto di lavoro.

Gestione della posta elettronica

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

- l'indirizzo del destinatario sia stato correttamente digitato;
- l'oggetto del messaggio non contenga direttamente il riferimento a stati, fatti o qualità idonei a rivelare dati di natura sensibile;
- nel corpo del messaggio sia indicata la riservatezza del messaggio.

Salvataggio di dati

Con cadenza quotidiana la Società esegue il salvataggio dei dati trattati utilizzando le misure e gli apparati a ciò destinati.

Tutti gli eventuali supporti di memorizzazione devono essere sottoposti a scansione antivirus.

MISURE PER TRATTAMENTO DI DATI EFFETTUATI CON ATTI E DOCUMENTI CARTACEI

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

- verificare che siano rispettati i criteri di controllo e custodia per tutto il ciclo di lavorazione necessario allo svolgimento delle operazioni di trattamento effettuate tramite atti e/o documenti; in particolare qualora i documenti contenenti i dati personali siano affidati direttamente all'incaricato, questo è tenuto a controllarli e custodirli in modo da impedire l'accesso a persone non autorizzate fino alla restituzione all'esito delle operazioni di trattamento effettuate;
- L'accesso agli archivi contenenti dati personali deve essere controllato; chi vi accede dopo l'orario di lavoro a qualsiasi titolo deve essere preventivamente autorizzato;
- Nel caso in cui sia necessario effettuare trasmissioni o riproduzione di documenti contenenti dati personali devono essere adottate le successive cautele:

  NON lasciare incustoditi presso fax, stampanti e fotocopiatrici documenti contenenti dati personali;

  In caso di trasmissione via fax di documenti contenenti dati personali verificare, eventualmente per via telefonica, l'avvenuta ricezione del fax e, una volta trasmessi ritirarli immediatamente;

  segnalare eventuali malfunzionamenti di strumenti elettronici

FUNZIONI DI CONTROLLO E VIGILANZA NEI CONFRONTI DI FORNITORI DI STRUMENTI ELETTRONICI E

DI ADDETTI ESTERNI ALLA GESTIONE E MANUTENZIONE DI STRUMENTI ELETTRONICI:

a) in occasione di ciascun intervento di manutenzione e di assistenza tecnica, verificare che sia rilasciato un verbale sulla esecuzione dei lavori, che attesti la conformità alle regole contenute nel presente Regolamento;

b) accertare che i software operativi e i programmi applicativi siano idonei ad assicurare:

- la separazione tra dati anagrafici e dati sensibili;

- la tracciabilità delle attività degli utenti, nel rispetto del codice privacy e delle garanzie di tutela dei dipendenti;

- un sistema di autenticazione e di autorizzazione conforme alla normativa in materia di protezione dei dati personali;

FUNZIONI DI CONTROLLO E DI VIGILANZA DA PORRE IN ESSERE AL FINE DI UNA CORRETTA GESTIONE DELLA

PRIVACY AZIENDALE (RESPONSABILE DI FUNZIONE):

a) verificare l'adozione di misure di sicurezza idonee in relazione al trattamento dati personali;

b) verificare gli eventi che hanno causato rischi per l'integrità e la disponibilità dei dati personali;

c) pianificare attività di audit interno, finalizzata al controllo del rispetto delle istruzioni operative e delle misure di sicurezza;

d) verificare il rispetto delle istruzioni impartite ai responsabili e agli incaricati del trattamento/addetti alla manutenzione;

e) verificare periodicamente la congruità ed efficienza delle misure di sicurezza perseguendo l'obiettivo di raggiungere un livello di protezione idoneo in relazione alle disposizioni vigenti;

f) comunicare a tutti gli incaricati del trattamento/addetti alla manutenzione le misure da predisporre e/o rispettare per la protezione dei dati di loro competenza;

g) in caso di violazione dei dati (data breach) effettuare entro 72 ore l'opportuna comunicazione al Garante Privacy ed agli interessati a norme del GDPR;

h) gestire l'assegnazione delle credenziali di autenticazione ai soggetti incaricati del trattamento;

i) provvedere alla disattivazione/variazione delle utenze, ivi compreso l'account di posta elettronica, assegnate al personale cessato dal servizio o che abbia modificato il proprio ambito di trattamento.

ISTRUZIONI PER L'ACCESSO AGLI ADDETTI ALLA MANUTENZIONE

L'accesso agli addetti alla gestione e manutenzione del sistema informatico è consentito unicamente ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere alle operazioni di manutenzione dei programmi o del sistema informatico.

A ciascun addetto alla manutenzione, previa sottoscrizione di apposito atto per accettazione, è pertanto consentito eseguire le operazioni strettamente necessarie a tali scopi e/o richieste dal titolare, secondo le seguenti istruzioni operative:

- Nel caso in cui sia necessario effettuare stampe di prova per controllare il funzionamento di stampanti o per verificare il funzionamento di strumenti o programmi installati, non utilizzare file già esistenti ma creare file di prova.

- Nel caso si renda strettamente necessario accedere a file contenenti dati (ad esempio per il recupero di un testo) limitare l'accesso ai dati per il tempo strettamente necessario all'assolvimento delle operazioni di manutenzione.
- Per effettuare operazioni di manutenzione sui database aziendali che prevedano la raccolta e la conservazione dei dati, tali dati dovranno essere custoditi in modo tale da non essere accessibili da soggetti non autorizzati.
- Devono inoltre essere adottate le misure di sicurezza minime previste dal codice in materia di protezione dei dati personali;

- E’ necessario informare al più presto il titolare o il responsabile del trattamento qualora si dovessero riscontrare malfunzionamenti o non conformità.
- Tutti i dati personali contenuti nei data base devono essere protetti da password;
- Nel caso in cui sia necessario accedere ai dati attraverso gli strumenti elettronici in dotazione agli incaricati, attenersi alle seguenti indicazioni:

o in presenza dell’incaricato, far digitare la password dall’incaricato stesso evitando di venirne a conoscenza;

o in assenza dell’incaricato rivolgersi alla persona individuata dall’incaricato quale proprio fiduciario il quale provvederà all’inserimento della password.

- Nei casi in cui sia necessario accedere ai dati personali attraverso il server, rivolgersi al responsabile di funzione o provvedere, in collaborazione con il responsabile di funzione stesso, alla creazione di credenziali di autenticazione da utilizzarsi esclusivamente per l’accesso da parte degli addetti alla manutenzione/gestione dei sistemi informatici;
- Il responsabile di funzione ha facoltà, in qualunque momento di controllare e verificare l’operato degli addetti alla manutenzione;
- Qualora si renda necessario prelevare apparecchiature elettroniche per effettuare attività di ripristino o interventi di manutenzione che comportino il reset di password precedentemente individuate, la nuova password di accesso sarà comunicata all’incaricato il quale provvederà a cambiarla al termine delle operazioni di manutenzione;
- E’ assolutamente vietato comunicare o diffondere i dati personali di qualsiasi natura provenienti dai database gestiti dalla società, se non previa espressa comunicazione scritta;
- In caso di accesso in remoto, previamente autorizzato, deve sempre essere presente l’incaricato addetto alla postazione interessata dall’intervento. Al riguardo è vietato creare una cartella contenente password