CADIAI 50 Una storia di cura e di lavoro

DELIBERATO DAL C.D.A.
IN DATA 19 MAR 2024

CHILD SAFEGUARDING POLICY

CADIAI è una cooperativa sociale che eroga servizi socio-sanitari ed educativi e fornisce servizi di sorveglianza sanitaria, di sicurezza dei lavoratori e formazione sulla sicurezza alle aziende. È iscritta al registro delle ONLUS (organizzazioni non lucrative di utilità sociale). CADIAI è nata il 30 settembre del 1974 e da allora opera prevalentemente nella provincia di Bologna, territorio in cui è storicamente radicata e nel quale è in grado di valorizzare al meglio i legami creati nel corso degli anni con le diverse comunità locali.

Gli ambiti di attività nei quali CADIAI opera sono i seguenti:

- Servizi per persone non autosufficienti: assistenza domiciliare, servizi territoriali, diurni e residenziali per anziani e per persone adulte con disabilità.
- Servizi per la prima infanzia, la scuola, gli adolescenti: nidi e scuole dell'infanzia; centri genitori-bambini;
- servizi di integrazione scolastica per bambini e ragazzi con disabilità; servizi per bambini e ragazzi con disagio psichico; gruppi educativi e interventi territoriali.
- Servizi di prevenzione e protezione rivolti alle aziende: sorveglianza sanitaria; sicurezza degli ambienti di lavoro; formazione sulla sicurezza.

CADIAI da sempre mette in campo risorse e processi che assicurino il presidio costante degli aspetti qualitativi dei servizi, essendo consapevoli che la qualità non è un livello organizzativo che si possa raggiungere una volta per tutte, ma è un fattore dinamico di adattamento progressivo all'evoluzione del bisogno e del contesto socio culturale di riferimento.

STATEMENT

Come parte del nostro impegno per la qualità dei servizi offerti, riconosciamo l'importanza di integrare la protezione dell'infanzia nel nostro sistema di gestione aziendale.

La Child Safeguarding Policy svolge un ruolo essenziale nel perseguire la mission di CADIAI di soddisfare al meglio i bisogni dei minori, creando un ambiente sicuro e protetto in cui possano crescere e svilupparsi in modo sano e positivo. La nostra cooperativa sociale si impegna a garantire che tutti i bambini e le bambine con cui interagiamo siano al sicuro da qualsiasi forma di danno, abuso o trascuratezza. Questo impegno riflette il nostro obiettivo di promuovere il benessere dei minori e di

fornire loro le migliori opportunità possibili per il loro sviluppo fisico, emotivo e cognitivo. Attraverso la Child Safeguarding Policy, ci impegniamo a fornire linee guida chiare e procedure efficaci per proteggere i diritti e la sicurezza dei minori, contribuendo così a costruire una comunità in cui ogni bambino e bambina possa crescere felice, sana e protetta.

Obiettivi

La nostra Child Protection Policy:

- Considera la prevenzione, protezione e promozione dei diritti all'infanzia una priorità;
- Considera la tutela della riservatezza quale adempimento normativo e quale standard qualitativo nelle situazioni di potenziale rischio;
- Promuove nei propri servizi, progetti, azioni, collaborazioni un approccio gentile, rispettoso, equilibrato, alla giusta vicinanza nei confronti dei propri utenti, di minore età e non solo;
- Assicura il rispetto delle persone coinvolte nelle proprie attività, dei minorenni nonché delle stesse socie e soci, operatrici ed operatori, dipendenti, collaboratrici e collaboratori quale dimensione preliminare;
- Rispetta punti di vista, voci, necessità e facilita l'emersione degli stessi in una chiave di advocacy concreta, funzionale, non invasiva, tutelante al fine di valorizzare attivazione autonoma e non ledere alcun diritto individuale;
- Promuove il benessere delle bambine e dei bambini in tutti i contesti professionali in cui CADIAI è coinvolta;
- Promuove verso i propri partners, stakeholders, committenti i principi della Policy stessa

La Child Safeguarding Policy di CADIAI è accompagnata da un disciplinare adottato da tutti i professionisti coinvolti, sottoscritto annualmente.

Maltrattamento e Abuso all'Infanzia

CADIAI adotta La Convenzione dei Diritti del Fanciullo ONU quale documento primario.
La policy di CADIAI si ispira ai principi del network internazionale Keeping Children Safe, fa riferimento alle classificazioni internazionali di ISPCAN, la società Internazionale di Prevenzione contro Abuso e Maltrattamento e utilizza la cornice istituzionale dell'Autorità Garante dei Diritti dell'Infanzia e dell'Adolescenza, Presidenza del Consiglio dei Ministri quale framework puntuale sul tema.

Le classificazioni e gli aspetti normativi nazionali che fanno da corollario legislativo nonché metodologico sono definiti dagli Allegati 1 e 2, in una trattazione ampia e puntuale al fine di poter contenere quanto più possibile lo scenario nazionale e rappresentarne le tipologie e le azioni preventive, protettive e di tutela del nostro Paese.

Commissione Etica

La Child Safeguarding Policy è inoltre strettamente allineata ai principi etici e alle direttive delineate nel Codice Etico CADIAI – ovvero l'enunciazione dell'insieme dei diritti, dei doveri e delle responsabilità della Cooperativa rispetto a tutti i soggetti con i quali entra in relazione per il conseguimento del proprio oggetto sociale (soci, dipendenti e collaboratori, utenti, clienti, fornitori, organi di controllo, istituzioni, collettività). Riconosciamo che la protezione dei bambini e delle bambine è una responsabilità prioritaria che deve guidare tutte le nostre azioni e decisioni.

Il Codice Etico CADIAI sottolinea l'importanza dell'integrità, della trasparenza e del rispetto dei diritti umani in tutte le nostre attività. La Child Safeguarding Policy si allinea a questi principi, impegnandoci a fornire un ambiente sicuro e protetto per tutti i bambini e le bambine con cui entriamo in contatto.

Inoltre, il Codice Etico CADIAI richiede il rispetto delle leggi e delle normative applicabili, nonché la promozione di una

cultura aziendale basata sull'equità e sull'empatia. La Child Safeguarding Policy si inserisce in questo contesto fornendo linee guida chiare e procedure per garantire il rispetto delle leggi e dei diritti dei bambini e delle bambine, così come per promuovere un ambiente in cui i bambini e le bambine possano crescere e svilupparsi in modo sano e sicuro.

Allo staff di CADIAI è richiesto di assumere i seguenti principi:

- Trattare bambine/i con rispetto riconoscendoli sempre come soggetti di diritto;
- Promuoversi attivamente nella affermazione e tutela dei diritti di bambine/i;
- Rispettare l'età evolutiva nei suoi diversi tempi, manifestazioni, contesti;
- Rispettare e accogliere le specificità, tutte, come dimensioni rappresentative e identitarie e non come diversità;
- Promuoversi nella valorizzazione del pensiero, parola, significazione da parte di bambine/i della propria esperienza di crescita;
- Promuoversi nell'informazione e trasmissione di conoscenza a bambine/i dei propri diritti;
- Promuoversi nel costruire opportunità per la valorizzazione dei talenti, abilità, potenzialità di bambine/i;
- Promuoversi nella costruzione di una piacevolezza e benessere nell'esperienza presso i differenti servizi;
- Prendersi cura degli ambienti e contesti, assicurandone la sicurezza e il benessere;

- Innovare i processi educativi tramite costante formazione e aggiornamento garantendo la massima qualità possibile in termini professionali;
- Accompagnare alla crescita e alla consapevolezza dei propri comportamenti non utilizzando per alcun motivo punizioni corporali o dimensioni punitive lesive per alcun motivo;
- Assumere una postura professionale accogliente, inclusiva, paziente nei confronti di qualsiasi situazioni possa occorrere;
- Adottare un linguaggio propositivo, accogliente, rispettoso, educato in ogni contesto;
- Tutelare costantemente la privacy di bambine/i in ogni situazione e/o circostanza.

CADIAI adotta una Policy specifica di protezione dei dati sensibili attraverso un puntuale disciplinare di Tutela della Privacy rivolta a dipendenti, collaboratori interni ed esterni, fornitori e utenti dei propri servizi di cui all'Allegato 3.

PROCEDURE

RECLUTAMENTO e FORMAZIONE

CADIAI adotta una prassi di reclutamento inserita nelle procedure di qualità dell'ente (Allegato 4) e rispondente ad una dimensione procedurale che prevede un accompagnamento/affiancamento iniziale del potenziale candidato, previa prima selezione e quindi una conoscenza puntuale, operativa, concreta, contestualizzata.

La selezione iniziale è strutturata in un colloquio conoscitivo, previa valutazione del curriculum vitae e dei titoli posseduti e a fronte dell'acquisizione di referenze specifiche dai contesti precedenti e indicati dal candidato nel curriculum vitae e nelle comunicazioni di autocandidatura e/o procedura di prima selezione.

Il colloquio conoscitivo è sempre condotto da figura apicale della cooperativa e indirizzato a conoscere competenze, esperienze, referenze e attitudine oltre ad una condivisione dei principi inderogabili di CADIAI.

Il profilo selezionato, in prima fase, affianca collaboratori esperti per un periodo concordato e viene inserito in contesti che possano vagliarne approccio e competenza, rispondenza alle necessità professionali ed etiche richieste.

Il profilo selezionato, dopo una fase di accompagnamento/affiancamento viene inserito nei piani formativi di CADIAI e

conseguentemente e/o parallelamente inserito lavorativamente.

Lo staff di CADIAI è costantemente e puntualmente formato ai temi tecnici sui diritti di bambine/i e ai temi della Policy.
CADIAI promuove formazione specialistica sui temi di abuso e maltrattamento a fronte delle tipologie di servizi e progetti attivati, internamente ed esternamente, promuovendo e sensibilizzando le tematiche della Policy verso il territorio.
CADIAI investe fortemente in formazione e in benessere dei propri operatori in chiave di prevenzione del burn-out e del miglior possesso di competenze possibili credendo fortemente nel ruolo operativo dei propri professionisti.

PROTEZIONE E SEGNALAZIONE

CADIAI in relazione all'allegato normativo della presente policy (Allegato 1) procede a norma di legge secondo quanto segue.

Le procedure di protezione e segnalazione e i principi ispiratori sono qui sinteticamente riproposti:

- I soggetti di minore età sono sempre informati dei loro diritti e tutelati e protetti da situazioni potenzialmente critiche;
- Tutti i progetti/servizi/interventi sostengono e promuovono una cultura della non violenza sotto tutti i punti di vista e manifestazioni, definendoli come inaccettabili, in ogni caso;
- Bambine/i vengono debitamente attrezzati ed equipaggiati per essere primi protagonisti nel processo di protezione, disclosure e segnalazione;
- Tutte le procedure che includono direttamente minorenni sono debitamente declinate con linguaggio semplice e comprensibile; CADIAI è formato alla comunicazione con il minorenne costantemente e in maniera specifica;
- Ogni membro dello staff di CADIAI è impegnato nel promuoversi quale adulto di riferimento agendo di conseguenza;
- Ogni membro dello staff deve, nelle fattispecie successivamente elencate, riferire immediatamente al suo coordinatore oppure direttamente ad un membro del Consiglio di Amministrazione;
- Il Consiglio di Amministrazione di CADIAI è direttamente responsabile per la gestione delle segnalazioni e delle conseguenti attivazioni necessarie. In specifico l'operatore segnala internamente e tempestivamente si definisce la modalità di segnalazione alle Autorità competenti.

Si procede alla definizione di una segnalazione, diretta o a supporto di altri enti/committenti a seconda della specifica competenza, nelle seguenti situazioni:

- Rilevazione e valutazione di qualunque abuso, sia esso sospettato o confermato;
- Qualora un operatore è testimone diretto e/o sospetta una potenziale situazione di pregiudizio;
- Qualora un operatore riceva una segnalazione a propria volta da parte di partners e collaboratori esterni;
- Qualora un operatore riceva, direttamente o indirettamente, testimonianza diretta, narrazione, disclosure da parte di un soggetto di minore età;

Nel caso in cui un minorenne confidi una situazione di pregiudizio e o di abuso nelle definizioni presenti in questa Policy è necessario rispettare quanto segue:

- Rispondere ad un principio di riservatezza e massima serietà e considerazione di quanto ricevuto;
- Deve essere immediatamente informato il proprio coordinatore, responsabile o un livello di Direzione o Presidenza;
- Il bambino/a deve essere ascoltato nel rispetto dei suoi tempi, della propria età evolutiva, del contesto di riferimento, delle proprie competenze cognitive, linguistiche, relazionali, sociali;
- Il bambino/a deve essere informato dell'utilizzo della testimonianza nelle fasi successive

Per la conduzione della raccolta testimoniale, il personale di CADIAI presenta profili debitamente formati, esperti ai quali fare riferimento e puntualmente incaricati delle audizioni protette in qualità di Ausiliario di Polizia Giudiziaria a livello territoriale. Ogni situazione riconducibile a quanto indicato deve coinvolgere i professionisti incaricati e laddove possibile fare riferimento all'équipe dedicata interna a CADIAI.

Nel caso in cui il sospetto/accusato sia interno all'organizzazione la segnalazione deve essere fatta al CDA come indicato o qualora coinvolgesse livelli dirigenziali puntuali, ad altro membro del CDA, Direttore Generale o Presidente.
CADIAI si impegna e impegna il proprio staff nel:

- Proteggere il bambino/a e fornire tutto il supporto di cui ha bisogno per quanto di competenza facilitando processi esterni di sostegno/supporto;
- Proteggere e supportare il contesto di riferimento della bambina/o qualora non direttamente coinvolto;
- Proteggere la persona che ha scoperto l'abuso;
- Evitare qualsivoglia contatto tra la persona accusata dell'abuso e bambine/i coinvolti;

- Adottare le misure opportune sulla base della decisione delle autorità competenti

MONITORAGGIO E REVISIONE

La CSP di CADIAI viene aggiornata costantemente a fronte di nuove disposizioni normative e nuovi protocolli o procedure interne adottate.

La policy è oggetto di monitoraggio e revisione da parte dell'équipe di CADIAI dedicate ai progetti e servizi di prevenzione tutela e protezione a cadenza annuale.

Appendice 1 - Principi e riferimenti normativi

I diritti delle persone di minore età si collocano all'interno dei diritti fondamentali dell'uomo, riconosciuti, oltre che nelle disposizioni nazionali, nei trattati e nelle dichiarazioni internazionali. Il primo strumento nazionale in assoluto che tutela i loro diritti è la Carta Costituzionale che li ricorda in alcuni articoli specifici: all'art. 3 sancisce che "Tutti i cittadini hanno pari dignità sociale e sono eguali davanti alla legge, senza distinzione di sesso, di razza, di lingua, di religione, di opinioni politiche, di condizioni personali e sociali. È compito della Repubblica rimuovere gli ostacoli di ordine economico e sociale, che, limitando di fatto la libertà e l'eguaglianza dei cittadini, impediscono il pieno sviluppo della persona umana e l'effettiva partecipazione di tutti i lavoratori all'organizzazione politica, economica e sociale del Paese." Questi principi trovano espressione e completamento in altri precetti costituzionali (quali, ad esempio, gli articoli 2, 4, 6, 21, 30, 34, 37, 51) e nei valori costitutivi del diritto internazionale ed europeo che proibisce ogni tipo di discriminazione.

I principi sopra menzionati trovano espressione e vengono ribaditi in diversi documenti internazionali ed europei. Per cominciare la Convenzione Internazionale per i diritti dell'infanzia e dell'adolescenza, approvata dall'Assemblea generale delle Nazioni Unite il 20 novembre 1989 e ratificata dall'Italia con legge del 27 maggio 1991, n. 176, la quale sancisce all'art. 19 comma 1: "Gli Stati parti adottano ogni misura legislativa, amministrativa, sociale ed educativa per tutelare il fanciullo contro ogni forma di violenza, di oltraggio o di brutalità fisiche o mentali, di abbandono o di negligenza, di maltrattamenti o di sfruttamento, compresa la violenza sessuale, per tutto il tempo in cui è affidato all'uno o all'altro, o ad entrambi, i suoi genitori, al suo rappresentante legale (o rappresentanti legali), oppure ad ogni altra persona che ha il suo affidamento" e all'art. 31 "Gli Stati parti riconoscono al fanciullo il diritto al riposo ed al tempo libero, di dedicarsi al gioco e ad attività ricreative proprie della sua età e di partecipare liberamente alla vita culturale ed artistica".

Da ciò si deduce che le persone di minore età sono soggetti di diritto. La condivisione di questo principio non solo spinge alla promozione della loro personalità e della loro partecipazione attiva in ogni situazione in cui si trovano coinvolti, ma anche alla loro protezione da ogni forma di violenza e abuso.

In considerazione delle conseguenze sulla salute mentale, fisica e riproduttiva delle e dei minorenni e sullo sviluppo dell'intera società, "la violenza sui minori non è un problema esclusivamente sociale e culturale, ma è un problema di salute pubblica", così come definita dall'Oms nel 2002. In effetti, la stessa Organizzazione Mondiale della Sanità, da molto tempo raccomanda a tutti gli Stati di dotarsi di un piano nazionale di prevenzione della violenza e di metodologie, strumenti, linee guida e progettazioni rigorose e scientifiche al fine di poter controllare e confrontare i risultati raggiunti e l'efficacia delle azioni.

Gli abusi e le violenze su persone di minore età, non solo sono un reato particolarmente grave, ma hanno pesanti conseguenze per le vittime. In molti casi le persone di minore età sono vittime di abusi e violenze commesse da persone che conoscono, di cui si fidano e da cui dipendono. Ciò rende tale reato particolarmente difficile da prevenire e identificare.

Un ulteriore documento giuridico di fondamentale importanza è la Convenzione del Consiglio d'Europa sulla prevenzione e la lotta contro la violenza nei confronti delle donne e la violenza domestica, sottoscritta a Istanbul l'11 maggio 2011, ratificata

dall'Italia con legge giugno 2013, n. 77, e in vigore dal 1° agosto 2014, la quale contiene norme di contrasto in materia di abusi sessuali su persone di minore età in ambito domestico.

Un passo importante in materia di contrasto agli abusi sessuali sulle persone di minore età è stato compiuto dall'Unione Europea nel 2011 con l'adozione della Direttiva 2011/93/UE del Parlamento Europeo e del Consiglio, la quale ha istituito norme minime relative alla definizione dei reati e delle sanzioni in materia di abuso e sfruttamento sessuale delle e dei minorenni e di materiale pedo-pornografico, e che comprende la prevenzione, l'indagine e il perseguimento dei reati, nonché l'assistenza e la protezione delle vittime.

L'esigenza di una più forte ed efficace tutela penale dei soggetti minorenni contro lo sfruttamento e gli abusi sessuali si è affermata con la ratifica da parte dell'Italia, attraverso la legge n. 172/2012, della Convenzione del Consiglio d'Europa sulla protezione dei minori dallo sfruttamento e dagli abusi sessuali, ossia la cosiddetta Convenzione di Lanzarote. Successivamente, il legislatore italiano ha recepito, con il d.lgs. del 15 dicembre 2015, n. 212, la Direttiva 2012/29/UE del Parlamento Europeo e del Consiglio, del 25 ottobre 2012 che istituisce norme minime in materia di diritti, assistenza e protezione delle vittime di reato.

La direttiva considera il reato come una violazione dei diritti individuali delle vittime e consolida il principio secondo il quale "le vittime di reato dovrebbero essere riconosciute e trattate in maniera rispettosa, sensibile e professionale, senza discriminazioni di sorta fondate su motivi quali razza, colore della pelle, origine etnica o sociale, caratteristiche genetiche, lingua, religione o convinzioni personali, opinioni politiche o di qualsiasi altra natura, appartenenza a una minoranza nazionale, patrimonio, nascita, disabilità, età, genere, espressione di genere, identità di genere, orientamento sessuale, status in materia di soggiorno o salute." Ulteriormente, la Commissione Europea, al fine di prevenire e contrastare la violenza e di rafforzare la protezione delle vittime di reato, ha emanato la Strategia Europea sui diritti delle vittime 2020-2025.

Ulteriori misure in materia di tutela della persona di minore età dagli abusi sessuali sono state adottate ultimamente a livello Europeo: la Strategia dell'UE per la sicurezza 2020-2025 e la Strategia dell'UE per una lotta più efficace contro gli abusi sessuali sui minori del 2020, le quali considerano la lotta contro gli abusi sessuali su minorenni un fattore primario e forniscono un quadro di riferimento per sviluppare una risposta efficace per contrastare e reprimere tale reato. Esse stabiliscono iniziative per attuare e sviluppare un quadro giuridico adeguato, rafforzare la risposta delle autorità di contrasto e favorire un'azione multidisciplinare coordinata in materia di prevenzione, indagine e assistenza alle vittime.

Tra le attuali iniziative adottate in materia di tutela delle persone di minore età si menziona anche la Risoluzione del Parlamento Europeo dell'11 marzo 2021 sui diritti dei minori alla luce della Strategia dell'Unione Europea sui diritti dei minori (2021/2523(RSP) che ai punti 13 e 14 invita gli Stati membri a "intensificare le proprie azioni per porre fine a tutte le forme di violenza e discriminazione nei confronti dei minori, comprese la violenza fisica, sessuale, le lesioni e gli abusi sessuali, ecc." Anche le Nazioni Unite nell'Agenda 2030 per lo sviluppo sostenibile, il programma d'azione per le persone, il pianeta e la prosperità sottoscritto nel settembre 2015 dai governi dei 193 Paesi membri dell'ONU, prevede nei suoi obiettivi 16.1 e 16.2 "la necessità di ridurre ovunque e in maniera significativa tutte le forme di violenza e porre fine all'abuso, allo sfruttamento,

al traffico di bambini e a tutte le forme di violenza e tortura nei loro confronti".

In Italia negli ultimi anni sono state introdotte significative modifiche al complesso della normativa vigente in materia di tutela delle persone di minore età da ogni forma di violenza. I comportamenti che integrano gli abusi, che possono essere fisici, psicologici e sessuali, e i maltrattamenti nei confronti di minorenni sono stati, nel tempo, nella normativa sovranazionale e nazionale, sempre più specificati e dettagliati non solo in termini di contenuto e sanzione, ma soprattutto in termini di prevenzione e formazione dei soggetti adulti che tali comportamenti possono prevenire, o comunque individuare precocemente al fine di determinarne l'immediata cessazione a tutela della vittima minorenne.

Nel nostro ordinamento le disposizioni normative del Codice Penale contemplano tutte le varie forme di abuso e maltrattamento.

Il 9 agosto del 2019 è entrata in vigore la legge n. 69 del 2019, recante «Modifiche al codice penale, al codice di procedura penale e altre disposizioni in materia di tutela delle vittime di violenza domestica e di genere» (c.d. "Codice Rosso") la quale oltre ad analizzare alcune delle modifiche normative apportate al codice penale, concentrando l'attenzione sulle nuove fattispecie di reato, mira a garantire e dare un'attuazione immediata alla protezione delle vittime predisponendo una corsia preferenziale.

In effetti, con l'adozione della normativa sono state introdotte nuove fattispecie di reato, tra le quali, in particolare, il reato di revenge-porn, ossia la diffusione illecita di immagini o video sessualmente espliciti senza il consenso delle persone rappresentate. Ha poi aumentato le sanzioni e le aggravanti per i reati già esistenti, quali omicidio, maltrattamenti contro familiari o conviventi, atti persecutori, violenza sessuale, anche di gruppo e atti sessuali con minorenni. Evidenzia, in particolare, la circostanza per cui la presenza della persona di minore età rappresenta sempre un'aggravante.

Di grande rilievo è stata l'approvazione della legge n. 47 del 2017 "Disposizioni in materia di misure di protezione dei minori stranieri non accompagnati", con l'obiettivo principale di rafforzare gli strumenti di tutela garantiti dall'ordinamento in loro favore. La legge n. 47/2017 ha introdotto misure che riguardano il rafforzamento dei diritti e delle tutele in favore di minorenni, a partire dalle fasi di accoglienza.

Degno di nota è la legge n. 71 del 29 maggio 2017 recante "Disposizioni a tutela dei minori per la prevenzione e il contrasto al fenomeno del cyberbullismo" che prevede una serie di misure volte a prevenire il fenomeno, in particolare all'art. 3 sancisce "l'istituzione di un tavolo tecnico per la prevenzione e il contrasto del cyberbullismo presso la Presidenza del Consiglio dei Ministri. Il tavolo tecnico, di cui al comma 1, coordinato dal Ministero dell'istruzione, dell'università e della ricerca, redige, entro sessanta giorni dal suo insediamento, un piano di azione integrato per il contrasto e la prevenzione del cyberbullismo, nel rispetto delle direttive europee in materia e nell'ambito del programma pluriennale dell'Unione europea."

Al fine di contrastare ogni forma di violenza nei confronti delle persone di minore età, apprezzabile è stata l'adozione del Decreto Legislativo n. 39 del 2014 in attuazione della Direttiva 2011/93/UE relativa alla lotta contro l'abuso e lo sfruttamento

sessuale dei minori e la pornografia minorile.
Per concludere, la violenza contro le persone di minore età è ancora frequente e ha effetti devastanti sulle vittime. Ancora oggi le risposte in materia sono insufficienti sia dal punto di vista sociale, culturale che normativo. Quindi si necessita di metodologie e strumenti condivisi, quali buone prassi e linee guida d'intervento adottate a livello locale, regionale e nazionale.
È necessario abbattere la cultura del silenzio, incoraggiare la denuncia del reato, venire incontro alle difficoltà della vittima e rafforzare ogni procedura che favorisca l'ascolto delle persone minorenni.
Occorre rivedere e modificare alcuni aspetti culturalmente accettati e/o considerati come "normali" o "approvati" per poter affrontare concretamente il fenomeno degli abusi, delle molestie e dei maltrattamenti.
La chiave per stabilire l'equilibrio non può che risiedere nella collaborazione, necessaria tra tutti i diversi livelli di governance. È pertanto fondamentale disporre di procedure chiare e uniformi per tutti gli organi deputati e chiamati a valutare quale sia, nel caso concreto, il superiore interesse della persona di minore età.

Di seguito l'elenco dei principali reati perseguibili d'Ufficio, ovvero quei reati di maggiore gravità, per i quali nel momento in cui un Pubblico Ministero venga a conoscenza di un'ipotesi di reato, deve iscriverla nel Registro Generale Notizia di Reato della Procura e avviare le indagini. L'azione che viene avviata d'ufficio è irrevocabile: non la si può dunque interrompere come avviene invece nel caso di remissione della querela.

Delitti "sessuali" (art. 609 bis e seguenti c.p.) a) Violenza sessuale commessa nei confronti di minore di anni 18; b) Violenza commessa dal genitore (anche adottivo) o dal di lui convivente, dal tutore o da persona alla quale il minore sia affidato per ragioni di cura, di educazione, di istruzione, di vigilanza o di custodia; c) Violenza sessuale di gruppo; d) Corruzione di minorenne (chi compie atti sessuali in presenza di un minore di 14 anni al fine di farlo assistere; chi fa assistere l'infra-quattordicenne ad atti sessuali o mostra materiale pornografico al fine di indurlo a compiere o subire atti sessuali); e)Adescamento di minorenni (chi allo scopo di commettere reati di prostituzione minorile, pornografia minorile, detenzione di materiale pornografico, violenza sessuale, …adesca un minore infra-sedicenne).
Prostituzione minorile (600 bis) Punisce chi recluta o induce alla prostituzione un minore di 18; favorisce, sfrutta, gestisce, …la prostituzione di un minore di 18 anni; chi compie atti sessuali con un minore tra i 14 e i 18 anni in cambio di corrispettivo di denaro o altra utilità, anche solo promessi.
Pornografia minorile materiale pedopornografico (art. 600 quater c.p.) Il presenti reati puniscono: chi utilizzando minori di anni diciotto, realizza esibizioni o spettacoli pornografici ovvero produce materiale pornografico; chi recluta, induce minori di anni diciotto a partecipare a tali esibizioni o ne trae profitto; chi anche con il mezzo telematico, distribuisce, divulga, pubblicizza notizie o informazioni finalizzate all'adescamento o allo sfruttamento sessuale di minori di 18 anni; chi assiste a

esibizioni o spettacoli pornografici in cui sono coinvolti minori di 18 anni; chi consapevolmente si procura, detiene, offre o cede ad altri, anche a titolo gratuito il materiale pornografico realizzato utilizzando minori di anni diciotto.

Minaccia (art. 612 c.p) Se qualcuno viene minacciato in modo grave (p.e. di morte) o con armi. Lesione personale* (art. 582 c.p.) Punisce chi procura lesione da cui deriva una malattia nel corpo o nella mente con prognosi superiore a 20 giorni o con circostanze aggravanti.

Stalking - atti persecutori (art 612 –bis) Chiunque, con condotte reiterate, minaccia o molesta un minore o una persona con disabilità (art.3 della legge 104/92) in modo da cagionare un perdurante e grave stato di ansia o di paura ovvero da ingenerare un fondato timore per l'incolumità propria o di un prossimo congiunto o di persona al medesimo legata da relazione affettiva, ovvero da costringere lo stesso ad alterare le proprie abitudini di vita.

Istigazione al suicidio (art. 580 c.p.) Chiunque determina altri al suicidio o rafforza l'altrui proposito di suicidio, ovvero ne agevola in qualsiasi modo l'esecuzione, è punito, se il suicidio avviene, con la reclusione da cinque a dodici anni. Se il suicidio non avviene, è punito con la reclusione da uno a cinque anni, sempre che dal tentativo di suicidio derivi una lesione personale grave o gravissima.

Violenza privata (art. 610 c.p.) Se una persona viene costretta con violenza o minaccia a fare, tollerare o omettere qualcosa (ad es. dover andare con qualcuno, ovvero non poter uscire ecc).

Delitti contro l'assistenza famigliare (artt. 570 e seg. c.p.)

a) Violazione degli obblighi di assistenza famigliare se commessi nei confronti di minori;

b) Abuso di mezzi di correzione o di disciplina;

c) Maltrattamenti in famiglia o verso i fanciulli.

La maggior parte dei reati sopra citati possono essere commessi anche on-line ovvero attraverso l'utilizzo di dispositivi connessi alla rete. Questa circostanza, che spesso rende più difficile l'individuazione del reato e più facile la sua attuazione da parte dei minori, può essere in alcuni casi una possibile aggravante del reato stesso. In questi casi, non essendoci reati specifici che descrivono questi comportamenti on-line, si deve fare riferimento ai reati sopra elencati. Ad esempio il Cyber-stalking, pur essendo un termine usato comunemente, non è un reato formalizzato nel codice penale e può essere ricondotto a più reati. Lo stesso vale per comportamenti come il Cyberbullismo e il Sexting che non sono descritti da un reato specifico, ma vanno valutati caso per caso in quanto possono includere uno o più dei reati perseguibili d'ufficio sopra elencati.

Appendice 2 – Definizioni, denominazioni e classificazioni

TERMINI E DEFINIZIONI

BAMBINO/A: l'art.1 della Convenzione delle Nazioni Unite sui diritti dell'infanzia (1989) definisce bambino/a ogni "essere umano avente un'età inferiore a diciott'anni".

TUTELA DEI BAMBINI/E: è la responsabilità di un'organizzazione di fare in modo che lo staff, le attività e i programmi non danneggino le/i minorenni, ovvero che non espongano i soggetti di minore età al rischio di danni e abusi e che eventuali problematiche dell'organizzazione relative alla sicurezza di bambine/i all'interno delle comunità in cui operano siano segnalate alle autorità competenti.
(Keeping Children Safe, International Child Safeguarding Standards).

ABUSO E MALTRATTAMENTO ALL'INFANZIA: si intendono tutte le forme di cattiva salute fisica e/o emozionale, abuso sessuale, trascuratezza o negligenza o sfruttamento commerciale o altro che comportano un pregiudizio reale o potenziale per la salute del/della bambino/a, per la sua sopravvivenza, per il suo sviluppo o per la sua dignità nell'ambito di una relazione caratterizzata da responsabilità, fiducia o potere (OMS 2002).

ABUSO FISICO
L'abuso fisico nei confronti di un bambino/a è quello che viene provocato (o che potrebbe essere provocato) da un'azione (o da una omissione) compiuta da chi ha nei suoi confronti un ruolo di responsabilità o di potere o di fiducia, come il genitore o figure ad essi equivalenti ed è causa di un danno.
Per maltrattamento fisico s'intende l'uso intenzionale della violenza fisica contro un/una minorenne che provoca o ha un'alta probabilità di provocare un danno per la salute, la sopravvivenza, lo sviluppo o la dignità, come aggressioni, punizioni corporali o gravi attentati all'integrità fisica, alla vita del bambino/a - adolescente. Si include il colpire, percuotere, prendere a calci, scuotere, mordere, strangolare, scottare, bruciare, avvelenare, soffocare. Gran parte della violenza a danno di minori dentro le mura domestiche viene inflitta con lo scopo di punire (WHO, 2006).
Bambine/i molto piccoli portatori di disabilità o che necessitano di cure speciali sono più vulnerabili al rischio di maltrattamento fisico, che si presenta spesso associato a isolamento sociale della famiglia, carenza di reti di sostegno, incuria e violenza psicologica. Non sempre il maltrattamento fisico lascia segni evidenti sul corpo del/della bambino/a e anche quando questi sono presenti, possono non essere facilmente visibili o immediatamente interpretabili in maniera corretta.

ABUSO PSICOLOGICO

L'abuso psicologico è causato dall'incapacità di offrire un ambiente appropriato al sostegno dello sviluppo del/della bambino/a, in cui sia presente una figura di riferimento affettivo, che gli permetta di esprimere appieno e in modo strutturato emozioni e relazioni, commisurate con il suo personale potenziale nel contesto della società in cui il/la bambino/a è inserito. Vi possono essere anche comportamenti nei confronti del/della bambino/a che possono causare, o avere una elevata possibilità di causare, danni al suo sviluppo psicologico, mentale, morale o sociale. Queste azioni ragionevolmente afferiscono alla persona che ha una relazione di responsabilità, fiducia o potere nei suoi confronti. Tali azioni includono: restrizioni della libertà di movimento; comportamenti sminuenti, denigratori, persecutori, minacciosi, spaventosi, discriminatori, ridicolizzanti, o altre forme di atteggiamento verbale ostile o di rifiuto.

Per maltrattamento psicologico, si intende una relazione emotiva caratterizzata da ripetute e continue pressioni psicologiche, ricatti affettivi, indifferenza, rifiuto, denigrazione e svalutazione che danneggiano o inibiscono lo sviluppo di competenze cognitivo - emotive fondamentali quali l'intelligenza, l'attenzione, la percezione, la memoria. È una forma molto insidiosa di violenza perché difficilmente rilevabile e può essere associata a altre forme di maltrattamento.

Il maltrattamento psicologico, nel tempo, mina profondamente la struttura di personalità in formazione, il senso di autostima del/della bambino/a e dell'adolescente, le sue competenze sociali e, più in generale, la sua rappresentazione del mondo. Rientra in questa categoria l'abuso e trascuratezza emozionale che implicano atteggiamenti trasversali nella relazione genitori figli (Glaser, 2002).

TRASCURATEZZA (NEGLECT)

La trascuratezza è la mancanza di supporto allo sviluppo del/della bambino/a in tutti gli ambiti: salute, educazione, emozione, crescita, nutrizione, accoglienza e condizioni di vita sicure, in rapporto alle risorse disponibili della famiglia o delle persone responsabili, mancanza che causa o può causare danno allo sviluppo psichico, mentale, spirituale morale o sociale del/della bambino/a. La trascuratezza si ravvisa anche nella mancanza di opportuna supervisione e protezione del bambino dalla violenza per quanto possibile.

ABUSO SESSUALE

L'abuso sessuale è il coinvolgimento del/della bambino/a in attività sessuali che non è in grado di comprendere appieno e per le quali non è in grado di poter esprimere un consenso o non è preparato, stante il suo grado di sviluppo, anche in assenza di leggi che considerino tali comportamenti come vietati. L'abuso sessuale di un bambino/a si sostanzia in una relazione di tipo sessuale tra un/una bambino/a e un adulto o un altro minorenne che per età o sviluppo è in una posizione di responsabilità, fiducia o potere verso il primo.

L'abuso sessuale può includere, pur non essendo limitato ad esso, le seguenti situazioni

Induzione o coercizione di un/una bambino/a volta a instaurare una attività sessuale contraria alla legge

Sfruttamento di un/una bambino/a in attività di prostituzione o altre pratiche sessuali contrarie alla legge
Sfruttamento di un/una bambino/a in attività pornografiche

Per abuso sessuale s'intende "Il coinvolgimento, intenzionale e interpersonale, di un/una minorenne in esperienze sessuali forzate o comunque inappropriate dal punto di vista dello stadio di sviluppo. Tali esperienze possono non comportare violenza esplicita o lesioni; possono avvenire senza contatto fisico e/o essere vissute come osservatori" (Cismai, 2015)

A seconda del rapporto esistente tra il/la bambino/a e l'abusante, l'abuso sessuale può suddividersi in:
1. intra-familiare, attuato da membri della famiglia nucleare o allargata;
2. peri-familiare, attuato da persone conosciute dal/dalla minorenne, comprese quelle a cui è affidato per ragioni di cura/educazione
3. extra-familiare, se l'abusante è una figura estranea all'ambiente familiare e al/alla minorenne
L'abuso sessuale è raramente un atto violento che lascia segni fisici. La valutazione medica rappresenta solo un aspetto spesso non dirimente di un complesso percorso diagnostico che deve necessariamente essere multidisciplinare. Di fronte al sospetto di abuso sessuale ricordiamo che in ogni caso la valutazione va fatta in modo esteso e complesso, analizzando almeno tre aree: segni fisici, psicologici, sociali oltre a racconti e affermazioni spontanee della presunta vittima. A fronte della frequente specificità sintomatologica sono particolarmente orientativi i comportamenti sessualizzati inadeguati per l'età dello sviluppo, soprattutto se caratterizzati da compulsività e pervasività.

SFRUTTAMENTO SESSUALE
Una particolare tipologia di abuso sessuale è rappresentata dallo sfruttamento sessuale. È il comportamento di chi percepisce danaro od altre utilità, da parte di singoli o di gruppi criminali organizzati, finalizzati all'esercizio di:
1. pedopornografia: ogni rappresentazione, con qualunque mezzo, di un/una minorenne in attività sessuali specifiche, reali o simulate, o qualunque rappresentazione degli organi sessuali di un minore per scopi principalmente sessuali;
2. prostituzione minorile: il/la minorenne è costretto a compiere atti sessuali in cambio di denaro o altra utilità;
3. turismo sessuale: si definisce "turista sessuale" colui che al fine di praticare sesso con i/le minorenni, organizza periodi di vacanza (o di lavoro) in paesi che, non solo tollerano la prostituzione minorile, ma spesso la propagandano per attirare il turista e incassare così valuta pregiata.

SFRUTTAMENTO
L'utilizzo commerciale o di altro tipo di un/una bambino/a ricorre quando il bambino viene impiegato per attività che portano beneficio ad altri.
Questo include – ma non è esclusivo – il lavoro minorile e la prostituzione minorile.

Queste attività danneggiano lo sviluppo psico - fisico, educativo, spirituale, morale socio – emotivo del/della bambino/a.

VIOLENZA ASSISTITA

Per violenza assistita da minorenni in ambito familiare si intende il fare esperienza da parte del/della bambino/bambina di qualsiasi forma di maltrattamento, compiuto attraverso atti di violenza fisica, verbale, psicologica, sessuale ed economica, su figure di riferimento o su altre figure affettivamente significative adulte e minorenni. Si includono le violenze messe in atto a livello intra-minorile e/o su altri membri della famiglia, gli abbandoni e i maltrattamenti ai danni di animali domestici.

Il/la bambino/a può fare esperienza di tali atti:
direttamente: quando avvengono nel suo campo percettivo;
indirettamente: quando ne è a conoscenza e/o ne percepisce gli effetti" (CISMAI)
La violenza assistita rappresenta un fattore di rischio altamente predittivo per le altre forme di maltrattamento.

ABUSO "ON LINE

Per abuso "on line" si intende ogni forma di abuso sessuale su minorenni perpetrata attraverso internet e la documentazione di immagini, video, registrazioni di attività sessuali esplicite, reali o simulate. Le forme di abuso sessuale online nei confronti di minorenni comprendono:

1. abuso sessuale off line documentato con video/immagini e diffuso in rete;
2. adescamento (grooming), si verifica quando l'adulto, con modalità manipolatorie, induce il/la minorenne a instaurare una relazione istigandolo a compiere atti sessuali online e/o a ottenere un incontro sessuale off line;
3. cybersex, in cui l'adulto e il/la minorenne compiono azioni sessuali esclusivamente via web;
4. sexting, nel quale due o più minorenni producono e si scambiano consensualmente messaggi, immagini o video di tipo sessuale che, se diffusi dagli stessi o da altri/e minorenni via internet o cellulari, possono essere utilizzati da adulti abusanti.

BULLISMO E CYBERBULLISMO

Con il termine bullismo si definisce la violenza tra pari, un fenomeno diffuso soprattutto nei contesti scolastici, tra adolescenti che mettono in atto varie forme di prevaricazione per manifestare il proprio desiderio di dominio nei confronti di coetanei più deboli.

Innanzitutto, tutti gli studi sul fenomeno hanno messo in evidenza come, per essere definita tale, la violenza tra pari debba necessariamente essere connotata da tre elementi: Asimmetria della relazione: deve essere presente uno squilibrio nel rapporto di forza tra il/la ragazzo/a che subisce l'azione violenta e il/la ragazzo/a, o gruppo di ragazzi/e, che agisce bullismo. Il bullismo è, prima ancora che un atto aggressivo, una dinamica relazionale in cui vi è uno squilibrio di potere.

Intenzionalità: il/la ragazzo/a o il gruppo di pari che si trova in una posizione di maggior forza rispetto al/alla compagno/a si

avvale della propria superiorità per infliggere un danno al/alla più debole, attraverso atti aggressivi intenzionali di varia natura. Non sempre questa intenzionalità indica la piena consapevolezza emotiva di ciò che si provoca nell'altro: in molti casi, infatti, la mancanza di empatia concorre al verificarsi di episodi di cyberbullismo tra gli adolescenti. Persistenza: sebbene anche un singolo episodio possa essere considerato come una forma di prevaricazione violenta, è più opportuno parlare di bullismo quando questo tipo di relazione persiste nel tempo e, se possibile, risulta essere organizzato, nel senso che l'iniziatore della violenza pianifica l'azione con grande meticolosità.

Va evidenziato, tuttavia, che, con l'evolversi delle nuove tecnologie e con le nuove modalità di comunicazione e relazione apprese dai/dalle ragazzi/e, il fenomeno delle prevaricazioni tra pari sembra aver assunto connotazioni sempre più specifiche. In particolare, l'evolversi delle nuove tecnologie ha messo in luce un fenomeno tutto nuovo di prevaricazione tra pari, già molto diffuso ed estremamente complesso, ossia il cyberbullismo. L'utilizzo di metodi e strumenti differenti deriva dalla capacità di utilizzo delle diverse tecnologie di chi commette l'azione di cyberbullismo, nonché dall'opportunità di impunibilità offerta dall'anonimato: tramite la mancanza di visibilità, il/la ragazzo/a violento pensa di molestare e perseguitare senza poter mai essere scoperto, barricandosi dietro la cosiddetta mask of electronic anonymity.

Il bullismo elettronico presenta sicuramente percorsi di rischio comuni al bullismo tradizionale, ma anche specifiche peculiarità, che ne mettono in evidenza le differenze e le analogie. Alcune caratteristiche della violenza on-line, quali la possibilità di mantenere l'anonimato, l'immediatezza nell'attuazione della prevaricazione, la raggiungibilità della vittima, l'assenza di una specifica temporalità tra l'azione di bullismo e la ricezione da parte della vittima, la possibilità di diffusione dell'atto di bullismo, costituiscono elementi di diversità rispetto alla prevaricazione nella quotidianità in presenza. A loro volta, questi elementi spiegano la pervasività di tali comportamenti e concorrono ad avere un impatto particolarmente negativo sulla tenuta emotiva del singolo che si ritrova a sentirsi impotente, impossibilitato a fermare le aggressioni e consapevole del fatto che la violenza potrà essere condivisa con moltissime persone.

Tra le principali manifestazioni di forme di violenza tra pari emergono:

Bullismo e intimidazione: comportamenti come schernire, perseguitare, ridicolizzare e umiliare, che rischiano di ledere la dignità di un/una bambino/a e/o farlo sentire intimidito o umiliato, e/o creano un ambiente ostile e spiacevole. Comprende anche esperienze di bullismo basate sul pregiudizio, quali razzismo e altre forme di discriminazione.

Abuso fisico: picchiare, strattonare, mordere, tirare i capelli oppure causare altri danni a livello fisico.

Bullismo e molestie online/cyberbullismo: usare telefoni, messaggi, e-mail, chat o social network per molestare, denigrare, minacciare, intimidire, schernire e ridicolizzare qualcuno. Fra le principali forme di cyberbullismo rientrano:

Cyberbashing o Happy Slapping: ha inizio nella vita reale, la vittima viene aggredita o molestata mentre altri riprendono la scena con lo smartphone, per proseguire su Internet, dove una volta che questi video vengono postati, chiunque è libero di condividerli, commentarli o aggiungere una reazione (es. like).

Exclusion: escludere intenzionalmente un/una coetaneo/a da un gruppo online ("lista di amici"), da una chat, da un videogame o da altri ambienti virtuali o isolarlo nel mondo reale con la finalità di infliggere sofferenza.

Hate Speech: l'utilizzo di un linguaggio violento, con contenuti a sfondo razzista o di incitamento all'odio sia off line sia sulle piattaforme digitali.

Sexting: unione tra le parole sexual e texting, indica l'invio di immagini e messaggi con esplicito riferimento sessuale attraverso smartphone o PC, con diffusione su app di messaggistica e/o social network.

Molestie sessuali: possono essere definite come comportamenti indesiderati di natura sessuale. Includono commenti di natura sessuale, ad es. commenti volgari, storielle, osservazioni, riferimenti o "battute" a sfondo sessuale, che magari si soffermano sull'abbigliamento e sull'aspetto fisico, oppure provocazioni. Rientrano in questa categoria anche eventuali azioni che possono suscitare in bambini/e e ragazzi/e sentimenti di intimidazione o umiliazione e/o che possono creare un ambiente ostile, offensivo o sessualizzato.

Abuso sessuale: comportamento dannoso a livello sessuale che può comprendere, ad es. aggressione sessuale/stupro, sollecitazioni o contatto fisico di natura sessuale inopportuni o indesiderati, forme di coercizione sessuale, insulti sessisti e uso di un linguaggio sessuale inappropriato.

I luoghi virtuali più vissuti dai/dalle minorenni sono: le live chat e la messaggistica, i social networks, le piattaforme musicali e di video sharing, nonché i videogame online. La percezione erronea di social e chat come luoghi privati porta i/le ragazzi/e ad inviare foto o video con contenuti a sfondo sessuale con leggerezza e senza riflettere sulle conseguenze che tale azione comporta. Il pericolo del sexting è il non controllo della propria immagine e della sua diffusione e la perdita della propria intimità a fronte di un'esposizione mediatica: il materiale che doveva rimanere privato comincia invece a circolare e diventa oggetto pubblico. Si configura, così, una dinamica fin troppo nota: uno dei due ragazzi coinvolti può tradire la fiducia dell'altro e la cassa di risonanza fornita da Internet crea un pubblico che alimenta la "vittimizzazione" di colui o colei le cui immagini sono state rese pubbliche senza il proprio consenso.

Il bullismo come tale non è un'ipotesi di reato prevista nel nostro ordinamento penale ma i reati che possono configurare il reato di bullismo sono molteplici, a seconda di come si esprime il comportamento (esempi: reato di minaccia, estorsione, violenza aggravata, etc.)

REATI PREVISTI DAL CODICE ROSSO

Sulla G.U. del 25 luglio 2019 è stata pubblicata la Legge 19 luglio 2019, n. 69 (recante "Modifiche al codice penale, al codice di procedura penale e altre disposizioni in materia di tutela delle vittime di violenza domestica e di genere") denominata "Codice Rosso", che avrà vigenza dal 9 agosto. Il testo include incisive disposizioni di diritto penale sostanziale, così come ulteriori di indole processuale. Nel Codice penale la legge in questione inserisce ben 4 nuovi reati:

il delitto di diffusione illecita di immagini o video sessualmente espliciti senza il consenso delle persone rappresentate (cd. Revenge porn), punito con la reclusione da uno a sei anni e la multa da 5mila a 15mila euro: la pena si applica anche a chi, avendo ricevuto o comunque acquisito le immagini o i video, li diffonde a sua volta per provocare un danno agli interessati.

La condotta può essere commessa da chiunque, dopo averli realizzati o sottratti, diffonde, senza il consenso delle persone interessate, immagini o video sessualmente espliciti, destinati a rimanere privati. La fattispecie aggravata se i fatti sono commessi nell'ambito di una relazione affettiva, anche cessata, ovvero mediante l'impiego di strumenti informatici;

il reato di deformazione dell'aspetto della persona mediante lesioni permanenti al viso, sanzionato con la reclusione da otto a 14 anni. Quando, per effetto del delitto in questione, si provoca la morte della vittima, la pena è l'ergastolo;

il reato di costrizione o induzione al matrimonio, punito con la reclusione da uno a cinque anni. La fattispecie è aggravata quando il reato è commesso a danno di minori e si procede anche quando il fatto è commesso all'estero da o in danno di un cittadino italiano o di uno straniero residente in Italia;

violazione dei provvedimenti di allontanamento dalla casa familiare e del divieto di avvicinamento ai luoghi frequentati dalla persona offesa, sanzionato con la detenzione da sei mesi a tre anni.

Appendice 3 – Privacy policy

PRIVACY

I Regolamenti di CADIAI:

- Norme comportamentali
- Policy IT

CADIAI
COOPERATIVA SOCIALE

28 12 2023 – Rev. 3

PRIVACY

Principi e norme comportamentali

CADIAI
COOPERATIVA SOCIALE

INDICE

INTRODUZIONE

Il Regolamento di CADIAI sulla protezione dei dati è teso ad assicurare il rispetto della legge, a prevenire violazioni di dati (c.d. data breach) e definisce le modalità in cui i dati personali devono essere trattati (raccolti, archiviati, resi sicuri, trasferiti e distrutti). Si applica a tutte le persone che lavorano per, o per conto di, CADIAI sotto ogni forma, incluso:

- dipendenti;
- amministratori;
- lavoratori interinali;
- liberi professionisti (infermieri, medici, tecnici, fisioterapisti, ecc.);
- tirocinanti.

Tutti i soggetti suindicati sono tenuti a rispettare il presente Regolamento quando trattano dati personali per conto di CADIAI.
Per domande o commenti si prega di contattare il Responsabile della Protezione dei Dati dpo@cadiai.it.

DEFINIZIONI

CONSENSO - 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.

DATI PERSONALI - Qualsiasi informazione riguardante una persona fisica identificata o identificabile; si considera identificabile la persona fisica che può essere 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.
I dati personali (di dipendenti, utenti/clienti, fornitori, ecc.) trattati da CADIAI riguardano a titolo esemplificativo ma non esaustivo:

- dati di contatto personali, tra cui nome, titolo, indirizzi, numeri di telefono e indirizzi email;
- data di nascita;
- stato civile;
- dati sui conti bancari;
- dati sulle buste paga;
- dati della patente di guida;
- dati sindacali;
- esperienza lavorativa (tra cui funzioni, percorso professionale, ore lavorative, formazione e appartenenza ad associazioni professionali);
- informazioni su provvedimenti disciplinari;
- sistemi di videosorveglianza;
- fotografie;
- dati sensibili di utenti.

DATI PERSONALI SENSIBILI - Informazioni che rivelano l'etnia, le opinioni politiche, le convinzioni religiose o simili, l'appartenenza sindacale, le condizioni di salute fisica o mentale, la vita sessuale, l'orientamento sessuale, i dati biometrici o genetici e i dati personali relativi a reati e condanne penali.

INFORMATIVA SULLA PRIVACY - Informativa sulle modalità del trattamento dei dati personali (artt.13-14 GDPR).

INTERESSATO - Qualsiasi informazione riguardante una persona fisica identificata o identificabile.

NORME GESTIONALI - I processi operativi di CADIAI relativi alle modalità di svolgimento delle operazioni di trattamento (norme gestionali sulla tenuta del registro dei trattamenti, sullo svolgimento delle valutazioni di impatto privacy, sulle figure privacy aziendali, ecc.).

PRIVACY FIN DALLA PROGETTAZIONE - L'adozione da parte del titolare di misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.

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.

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI (RGPD) O GENERAL DATA PROTECTION REGULATION (GDPR) - Il Regolamento Generale sulla Protezione dei dati dell'Unione Europea 2016/679.

RESPONSABILE DELLA PROTEZIONE DEI DATI (RPD)/DATA PROTECTION OFFICER (DPO)
La persona nominata responsabile della protezione dei dati ai sensi dell'art. 37 del Regolamento Europeo.

SEE - SPAZIO ECONOMICO EUROPEO (PAESI IN CUI VIGE IL REGOLAMENTO UE) - I 28 paesi dell'UE e Islanda, Liechtenstein e Norvegia.

TITOLARE DEL TRATTAMENTO - La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali. **CADIAI è il titolare del trattamento.**

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.

VALUTAZIONE D'IMPATTO PRIVACY O DATA PROTECTION IMPACT ASSESSMENT (DPIA) Processo valutativo effettuato dal titolare del trattamento (art. 35 GDPR) sugli effetti dei trattamenti sui dati personali.

VIOLAZIONE DI 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.

1. RESPONSABILITÀ

A CADIAI compete ai sensi dell'art. 24 GDPR la responsabilità giuridica della gestione dei dati personali tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.

CADIAI mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Queste misure sono riesaminate e aggiornate qualora necessario.

Il Responsabile della Protezione dei Dati (DPO) ha il dovere di vigilare sul presente regolamento e può essere contattato all'indirizzo dpo@cadiai.it.

È obbligatorio contattare il Responsabile della Protezione dei Dati nelle seguenti circostanze:

a) se non si è sicuri della base giuridica del trattamento;
b) se è necessario o meno raccogliere un esplicito consenso (ad es. in caso di raccolta di nuove banche dati, nuovi progetti, attività promozionali o commerciali, ecc.);
c) se si deve redigere un'Informativa sulla privacy (es. siti web, ecc.);
d) se non si è sicuri del periodo di conservazione applicabile ai dati personali che si stanno trattando;
e) se non si è sicuri di quali misure di sicurezza o di altro tipo devono essere adottate per proteggere i dati personali;
f) se vi è stata una violazione di dati personali (furto di hardware, file, credenziali, documenti, ecc.);
g) se non si è sicuri di quali siano le basi per il trasferimento dei dati personali al di fuori dall'Unione Europea;
h) se si riceve una richiesta e/o si ha bisogno di assistenza in merito a eventuali diritti avanzati da un interessato (se viene chiesta una cartella sanitaria, ecc.);
i) ogniqualvolta sia necessaria una Valutazione d'Impatto Privacy - PIA (ad es. in caso di apertura o modifica di servizi, acquisto nuovi gestionali/servizi, adozione di nuove procedure, ecc. – Vd. Paragrafo 11.3);
j) per chiedere consulenza quando si effettuano nuove attività di marketing diretto;
k) se si ha bisogno di assistenza con contratti o altri ambiti attinenti alla condivisione dei dati personali con terze parti.

2. PRINCIPI DI PROTEZIONE DEI DATI PERSONALI

CADIAI rispetta i principi relativi al trattamento dei dati personali stabiliti dal Regolamento Europeo che richiedono che i dati personali siano:

a) trattati in modo lecito, corretto e trasparente (liceità, correttezza e trasparenza);
b) raccolti solo per finalità determinate, esplicite e legittime (limitazione della finalità);
c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (minimizzazione dei dati);
d) esatti e ove necessario aggiornati (esattezza);
e) conservati in una forma che non consenta l'identificazione degli interessati per un arco di tempo superiore al conseguimento delle finalità per le quali sono trattati (limitazione della conservazione);
f) trattati in maniera da garantire la loro sicurezza mediante misure tecniche e organizzative idonee a proteggerli da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentale (sicurezza, integrità e riservatezza);
g) trasferiti in un altro paese previa verifica dell'esistenza di garanzie adeguate (limitazione del trasferimento);
h) messi a disposizione degli interessati, ai quali deve essere assicurato l'esercizio dei propri diritti (diritti degli interessati);
i) trattati in modo da garantire il rispetto dei diritti, le libertà fondamentali, la dignità nonché le manifestazioni legittime di volontà degli interessati, con particolare riguardo alle fasce deboli dei disabili, minori e anziani, soggetti che versano in particolare condizione di disagio e bisogno.

3. LICEITÀ, CORRETTEZZA E TRASPARENZA

3.1. LICEITÀ E CORRETTEZZA

CADIAI è autorizzata a raccogliere, trattare e condividere dati personali in modo corretto e lecito e per finalità specifiche. Il Regolamento Europeo limita le azioni attinenti ai dati personali alle finalità lecite specificate. Tali limitazioni non sono volte a impedire il trattamento, ma ad assicurare che il trattamento dei dati personali avvenga in modo corretto e non lesivo dell'interessato.
Il Regolamento Europeo consente il trattamento solo in presenza di una precisa base giuridica, alcune delle quali sono specificate di seguito:

- l'interessato ha fornito il consenso;
- il trattamento è necessario per l'esecuzione di un contratto con l'interessato;
- al fine di ottemperare all'adempimento di un obbligo legale;
- al fine di proteggere gli interessi vitali dell'interessato;
- al fine di proteggere i propri legittimi interessi laddove su questi ultimi non prevalgano interessi o diritti e libertà fondamentali dell'interessato.

In caso di mancato conferimento del consenso (ove facoltativo) l'incaricato darà tempestiva comunicazione agli uffici competenti della sede (Fatturazione, Personale, Comunicazione, Referente Privacy, ecc.).

3.2. CONSENSO

Un interessato acconsente al trattamento dei propri dati personali se indica il proprio consenso al trattamento in modo esplicito, mediante una dichiarazione o azione positiva – come la selezione di un'apposita casella.
Il consenso richiede un'azione affermativa, pertanto il silenzio, la preselezione di caselle o l'inattività non sono da considerarsi modalità idonee di acquisizione del consenso.
Qualora il consenso sia necessario quale base di liceità per il trattamento dei dati, gli interessati (es. utenti) devono essere messi in grado di revocare facilmente il proprio consenso in qualsiasi momento (es. newsletter).
Gli incaricati di CADIAI dovranno fornire la prova del consenso ricevuto e tenere traccia di tutti i consensi affinché CADIAI possa dimostrare l'ottemperanza al Regolamento Europeo (es. log consensi espressi sui siti web).

3.3. Trasparenza – Informativa sulla privacy

Ogniqualvolta CADIAI raccoglie dati personali direttamente dagli interessati e prima di iniziare il relativo trattamento, deve fornire all'interessato un'informativa sulla privacy contenente tutte le informazioni previste dal Regolamento Europeo.

I contenuti dell'informativa sono elencati in modo tassativo negli articoli 13, paragrafo 1, e 14, paragrafo 1, del regolamento UE 2016/67. In particolare, il titolare DEVE SEMPRE specificare i dati di contatto del DPO (Responsabile della Protezione Dati), la base giuridica del trattamento, l'interesse legittimo e se quest´ultimo costituisce la base giuridica del trattamento, nonché se trasferisce i dati personali in Paesi terzi e, in caso affermativo, attraverso quali strumenti (esempio: si tratta di un Paese terzo giudicato adeguato dalla Commissione Europea; si utilizzano norme vincolanti di gruppo; sono state inserite specifiche clausole contrattuali, ecc.).

Il Regolamento Europeo prevede anche ulteriori informazioni in quanto "necessarie per garantire un trattamento corretto e trasparente": in particolare, il titolare deve specificare il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione, e il diritto di presentare un reclamo all'autorità di controllo.

Se il trattamento comporta processi decisionali automatizzati e/o di profilazione, l'informativa deve specificarlo e deve indicare anche la logica di tali processi decisionali e le conseguenze previste per l'interessato.

Nel caso di dati personali non raccolti direttamente presso l'interessato l´informativa deve essere fornita entro un termine ragionevole che non può superare un mese dalla raccolta, oppure al momento della comunicazione (NON della registrazione) dei dati (a terzi o all'interessato).

4. Limitazione della finalità

I dati personali devono essere raccolti solo per finalità determinate, esplicite e legittime. Non devono inoltre essere trattati in alcuna maniera incompatibile con tali finalità.

5. MINIMIZZAZIONE DEI DATI

I dati personali devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati. Gli incaricati autorizzati al trattamento di CADIAI possono trattare dati personali solo quando necessario per l'espletamento delle rispettive mansioni. Quando i dati personali non sono più necessari per le finalità specificate, devono essere cancellati o anonimizzati in conformità con la Politica di conservazione dei dati di CADIAI.

6. ESATTEZZA

Il Regolamento Europeo prevede che i dati personali siano esatti e, ove necessario, aggiornati (fanno eccezione i c.d. "dati invarianti" come ad esempio la data di nascita). Devono essere corretti o cancellati senza ritardo quando inesatti. Ci si deve assicurare che i dati personali che si utilizzano e conservano siano esatti, completi, aggiornati e pertinenti per le finalità per cui sono stati raccolti. Si devono adottare tutte le misure ragionevoli per distruggere o rettificare dati personali inesatti o non più aggiornati.

7. CONSERVAZIONE DEI DATI

I dati personali non dovrebbero essere conservati in forma identificabile più a lungo di quanto necessario per la finalità del trattamento. Ove non vi sia più una finalità aziendale legittima per il trattamento dei dati, ad esempio per obblighi giuridici, contabili o di segnalazione, i dati personali devono essere cancellati o anonimizzati. La Politica di conservazione dei dati di CADIAI stabilisce i requisiti di conservazione (vd. Sistema Gestione Generale - Procedura Gestionale "Gestione Documenti").

8. INTEGRITÀ DELLA SICUREZZA E RISERVATEZZA

8.1. PROTEZIONE DEI DATI PERSONALI

Tutti coloro che trattano dati personali di CADIAI sono tenuti a seguire la Policy IT sull'uso degli strumenti informatici allegato al presente regolamento, di cui ne costituisce parte integrante, e seguire le seguenti norme comportamentali:

- non esporre dati riepilogativi di condizioni cliniche che potrebbero essere visibili a persone non autorizzate;
- custodire documenti contenenti dati personali in ambienti protetti (armadi, cassettiere, stanze chiuse a chiave o con badge, codici, ecc.);
- non creare duplicati delle chiavi di servizio ricevute;
- non portare fuori dalle sedi di lavoro documenti in formato cartaceo, salvo espressa e motivata autorizzazione e con le opportune precauzioni;
- in caso di consegna-ritiro dei dispositivi di accesso tenere un registro aggiornato;
- archiviare separatamente i dati sanitari in modo tale da non consentire un'indistinta consultazione nel corso delle normali attività amministrative**;**
- i dati sensibili e giudiziari non possono essere diffusi, e vanno comunicati solo a persone autorizzate;
- è vietata la diffusione con affissione in bacheche aziendali o con comunicazioni interne destinate alla collettività di dati personali riferiti ai lavoratori quali: motivazioni dell'assenza (es. permesso sindacale, adesione ad altre associazioni, visita medica, L 104, malattia, ferie, ecc.) ma indicazioni più generiche quali presenza/assenza;
- durante le spedizioni postali prestare la massima attenzione affinché sulla busta non siano riportati dati eccedenti (deve contenere solo mittente e destinatario ovvero nome della società) attraverso i quali sia possibile risalire (anche solo deducendoli), ai contenuti (es. prestazioni ricevute, tipologia di servizio di provenienza, ecc.);
- gli addetti alla ricezione di certificati medici o altri documenti attestanti la salute del lavoratore sono tenuti all'utilizzo delle sole informazioni necessarie e ad oscurare eventuali parti della documentazione (inviati per errore o per necessità) inerenti la diagnosi, la struttura dove è stata prestata assistenza (vd. visite mediche, ecc.);
- sui certificati medici legali che attestano l'idoneità al servizio di un lavoratore dovrà comparire solo la dicitura "idoneo" o "non idoneo" senza nessun riferimento a patologie sofferte ed essere messo a conoscenza esclusivamente della catena di responsabilità. Si precisa che il datore di lavoro non dovrà mai accedere in alcun modo ai dati sanitari del dipendente;

- l'uso di copie/fotocopie di atti/documenti contenenti dati personali, sensibili e/o giudiziari deve essere strettamente necessario e funzionale alle esigenze lavorative;
- eventuali fotocopie errate devono essere immediatamente distrutte in modo da rendere totalmente illeggibile ed irrecuperabile il documento;
- eventuali copie non possono essere usate come carta riciclabile o per appunti;
- i documenti cartacei contenenti dati personali vanno distrutti utilizzando i punti raccolta messi a disposizione per l'utilizzo della macchina distruggi-documenti;
- deve essere prestata attenzione affinché documenti contenenti dati sensibili non vengano lasciati nel fax, nello scanner, sulla fotocopiatrice, sul tavolo di altri colleghi o sul proprio in vista. Qualora siano presenti sulla scrivania dati sensibili o particolari (es. fascicoli e cartelle) si consiglia di voltarli al fine di evitare la presa visione a soggetti terzi non incaricati;
- non utilizzare il fax per l'invio di dati sensibili o personali, qualora sia strettamente necessario si chiede di:
  - anticipare l'invio del fax al destinatario per assicurarsi che sia il medesimo a riceverlo;
  - prestare attenzione alla corretta digitazione del numero cui inviare in documento;
  - utilizzare il modello fax predisposto con l'indicazione dell'appartenenza del documento;
  - non dimenticare documenti all'interno del fax;
- in caso di acquisizione di documenti in formato digitale da documentazione cartacea verificare che l'operazione avvenga correttamente e che il contenuto del documento oggetto di scansione sia correttamente leggibile al fine di evitare confusione di dati;
- controllare/adeguare periodicamente agli archivi cartacei in modo tale che non perdano la loro efficacia e funzionalità;
- è richiesto all'operatore di conservare con cura il suo cartellino di riconoscimento e, in caso di smarrimento e/o furto, di presentare denuncia alle forze dell'ordine e di avvisare tempestivamente il Coordinatore, l'Area di appartenenza, l'Ufficio Privacy, l'Ufficio Personale, l'Ufficio Amministrazione generale;
- le comunicazioni personali riferibili esclusivamente a singoli lavoratori devono avvenire con modalità tali da escludere l'indebita presa di conoscenza da parte di terzi o di soggetti non designati quali incaricati (ad esempio in busta chiusa con lembi sigillati e firmati o in alternativa piegando il documento e spillando i lati in modo da rendere illeggibile il contenuto);
- la comunicazione di dati sullo stato di salute deve essere resa nota all'interessato solo da soggetti legittimati per il tramite di un medico designato;

- in caso di violazione di dati personali (es. furto di un pc, smartphone, ecc.) si deve contattare tempestivamente prima di ogni iniziativa il Coordinatore del servizio, che a sua volta informerà l'Area di pertinenza, nonché l'Ufficio Privacy e l'Ufficio Gestione Sistemi Informativi;
- in caso di furto di dati (cartacei, strumentazioni, ecc.) le comunicazioni all'esterno devono essere effettuate dal Responsabile di Servizio all'Area, all'Ufficio Comunicazione e all'Ufficio Privacy per la verifica delle disposizioni impartite contrattualmente dal Titolare (es. Ente committente in caso di data breach).
  Anche le restanti comunicazioni (es. agli organi di stampa) devono essere indirizzate all'ufficio Comunicazione della Cooperativa: affinché esse siano sempre pertinenti, chiare e tempestive per rassicurare l'utenza rispetto alla qualità dei servizi, per tutelare la reputazione dell'organizzazione e ridurre l'impatto negativo, in termini di immagine.
  E' vietata infine la diffusione su social e chat di quanto accaduto per evitare ad esempio il rischio che la notizia raggiunga gli interessati prima che la Cooperativa li abbia potuti informare;
- analoga cautela ed attenzione dovrà essere riposta allorquando si trattino i dati in maniera non documentale ovvero durante colloqui diretti o durante l'uso dell'apparecchio telefonico (fisso o mobile): a tal proposito va assunto un timbro di voce adatto alle finalità del dato trattato ed adottare idonee misure di sicurezza, es. evitare l'utilizzo di ambienti promiscui, chiudere la porta, evitare la presenza di persone esterne e/o non autorizzate (o predisporre distanze di cortesia);
- non fornire a mezzo telefono dati ed informazioni di carattere sanitario o di natura riservata qualora non si conosca o non si abbia verosimilmente cognizione dell'identità o della legittimazione ad ottenere i dati richiesti del soggetto chiamante;
- prima di impostare una conversazione telefonica in vivavoce occorre avvertire ed avere il consenso di tutti gli interlocutori;
- sono vietate la registrazioni di telefonate ed incontri di lavoro senza il consenso degli interlocutori se non per utilizzo strettamente personale;
- prima di scattare foto e/o procedere a riprese audio e/o video informare sempre l'interessato ed accertarsi di averne acquisito la relativa liberatoria in forma scritta. Anche prima dell'utilizzo verificare se si dispongono le autorizzazioni necessarie (uso limitato al servizio, condivisione, diffusione, ecc.);
- l'operatore che, durante lo svolgimento delle proprie mansioni abbia contatti con il pubblico, è pregato di riceverlo in ambienti idonei (es. in ufficio, se necessario con scrivanie riparate, ecc.), chiedendo a chi resta in attesa di mantenere le distanze di cortesia;

- fare attenzione all'utilizzo di numeri non canonici, o servizi a pagamento, che vengono spesso utilizzati in buona fede (es. richieste di risposte telefoniche o fax ai numeri con prefissi 7xx o 9xx o 8xx).

8.2. SEGNALAZIONE DI UNA VIOLAZIONE DI DATI PERSONALI

Per "violazione di dati personali" si intende una 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.
Il Regolamento Europeo prevede che il titolare del trattamento ove possibile, entro 72 ore dalla scoperta, valuti se notificare la violazione all'Autorità Garante e in alcune circostanze all'interessato. Qualsiasi violazione deve essere comunicata tempestivamente telefonando al Responsabile Privacy Tel. 051/5283513 e scrivendo all'indirizzo email: dpo@cadiai.it.

9. LIMITAZIONE DEL TRASFERIMENTO

Il Regolamento Europeo limita il trasferimento dei dati a paesi esterni all'Unione Europea.

I dati personali possono essere trasferiti all'esterno dell'Unione Europea solo se prevale una delle seguenti condizioni:

a) il paese in cui CADIAI trasferisce i dati personali assicura un adeguato livello di protezione per i diritti e le libertà degli interessati;
b) sono presenti garanzie adeguate, tra cui norme vincolanti d'impresa (*Binding Corporate Rules*, BCR), clausole contrattuali modello standard approvate dalla Commissione Europea, un codice di condotta approvato o un meccanismo di certificazione;
c) l'interessato ha fornito l'esplicito consenso al proposto trasferimento dopo essere stato informato dei potenziali rischi; oppure (vedi punto "*d*");
d) il Regolamento Europeo chiarisce come sia lecito trasferire dati personali verso un Paese terzo non adeguato solo "per importanti motivi di interesse pubblico", in deroga al divieto generale, tuttavia deve trattarsi di un interesse pubblico riconosciuto dal diritto dello Stato membro del titolare o dal diritto dell´UE (si veda art. 49, paragrafo 4) – e dunque non può essere fatto valere l´interesse pubblico dello Stato terzo ricevente.

Di regola CADIAI non trasferisce dati all'esterno dell'Unione Europea. Eventuali proposte al riguardo devono essere rivolte preventivamente al Responsabile della Protezione dei Dati.

10. DIRITTI E RICHIESTE DELL'INTERESSATO

Gli interessati godono di una serie di diritti relativamente alle modalità in cui i loro dati personali sono trattati. Tali diritti includono:

a) revocare il consenso al trattamento in qualsiasi momento;
b) ricevere determinate informazioni sulle attività di trattamento del titolare;
c) esercitare il diritto di accesso ai propri dati personali detenuti da CADIAI;
d) impedire a CADIAI di utilizzare i dati personali che li riguardano a fini di marketing diretto;
e) richiedere a CADIAI di cancellare dati personali se non sono più necessari per le finalità per cui sono stati raccolti o trattati o rettificare dati inesatti o completare dati incompleti;
f) limitare il trattamento in specifiche circostanze;
g) essere informati di una violazione di dati personali suscettibile di causare un elevato rischio per i propri diritti e libertà;
h) presentare reclamo all'autorità di controllo; e (vedi punto i)
i) in limitate circostanze, ricevere o chiedere che i propri dati personali siano trasferiti a una terza parte in un formato strutturato, di uso comune e leggibile da dispositivo automatico.

Il termine per la risposta all'interessato è, per tutti i diritti (compreso il diritto di accesso), 1 mese, estendibili fino a 3 mesi in casi di particolare complessità; CADIAI deve comunque dare un riscontro all'interessato entro 1 mese dalla richiesta, anche in caso di diniego. Per ogni necessità va contattato il Responsabile della Protezione dei Dati.
L'apposita istanza per esercitare i suindicati diritti può essere scaricata dal sito dell'Autorità Garante (https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1089924).

11. RESPONSABILIZZAZIONE

CADIAI è responsabile del rispetto dei principi posti a protezione dei dati personali tramite risorse e controlli adeguati e deve essere in grado di dimostrarlo. CADIAI ottempera nei seguenti modi:

- nomina di un Responsabile della Protezione dei Dati (DPO) idoneamente qualificato;
- implementazione della "privacy fin dalla progettazione" nel trattamento di dati personali e conduzione di Valutazioni d'Impatto sulla Privacy quando il trattamento presenta un rischio elevato per i diritti dell'interessato;
- integrazione della protezione dei dati in documenti interni, tra cui il presente Regolamento Privacy, la Privacy Policy e le norme gestionali;
- formazione regolare dei lavoratori di CADIAI;
- svolgimento di audit periodici.

11.1. TENUTA DI REGISTRI E REGISTRO DEL TRATTAMENTO DEI DATI

Il Regolamento Europeo prevede che i titolari del trattamento tengano registri completi e accurati di tutte le attività di trattamento dei dati.
Il Registro del trattamento dei dati include il nome e i dati di contatto del titolare del trattamento e del Responsabile della Protezione dei Dati, chiare descrizioni dei tipi di dati personali, tipi di interessati, attività di trattamento, finalità di trattamento, destinatari terzi dei dati personali, località degli archivi dei dati personali, trasferimenti dei dati personali, periodo di conservazione dei dati personali e descrizione delle misure di sicurezza esistenti. Il Registro è tenuto presso la sede di CADIAI dal Referente Privacy e supervisionato dal DPO.

11.2. FORMAZIONE E CONTROLLI

CADIAI assicura a tutti i propri lavoratori un'adeguata formazione che consenta loro di rispettare le leggi sulla privacy. I sistemi e i processi di CADIAI sono sottoposti regolarmente a audit per valutarne l'idoneità.

11.3. VALUTAZIONE D'IMPATTO SULLA PRIVACY (DPIA)

I titolari del trattamento conducono Valutazioni d'Impatto sulla Privacy (DPIA) con la collaborazione del DPO quando implementano importanti programmi di modifica di sistemi o attività che coinvolgono il trattamento di dati personali, tra cui:

- l'utilizzo di nuove tecnologie (programmi, sistemi o processi) o la modifica di tecnologie (programmi, sistemi o processi);
- il trattamento automatico, inclusa la profilazione;
- il trattamento su larga scala di dati sensibili *(vedere di seguito);*
- la sorveglianza sistematica su larga scala di zone accessibili al pubblico.

11.4. Marketing diretto

L'Autorità Garante per la protezione dei dati personali ha precisato che è sufficiente richiedere all'interessato un unico consenso per attività riconducibili al marketing, come l'invio di materiale pubblicitario, di vendita diretta, di compimento di ricerche di mercato e di comunicazione commerciale.
Occorre però fare una distinzione tra comunicazioni commerciali (marketing) svolte in maniera tradizionale (posta cartacea, telefonate con operatore) o attraverso strumenti automatizzati (es. fax, sms, email, mms, telefonate preregistrate). Il consenso prestato per l'invio di comunicazioni commerciali tramite modalità automatizzate (come email o sms) copre anche quelle effettuate tramite posta cartacea o con telefonate tramite operatore.
Deve essere garantito il diritto di opposizione all'interessato in forma agevole e comprensibile. Se un cliente revoca il consenso in qualsiasi momento, i suoi dati devono essere eliminati appena possibile. L'eliminazione comporta la conservazione di informazioni appena sufficienti ad assicurare che le preferenze di marketing siano rispettate in futuro.

12. Modifiche del presente Regolamento

CADIAI si riserva il diritto di modificare il presente Regolamento sulla privacy in qualsiasi momento. La versione aggiornata è consultabile sulla piattaforma informatica aziendale "Zucchetti".

PRIVACY

Policy IT

CADIAI
COOPERATIVA SOCIALE

INDICE

DEFINIZIONI

Ai fini della presente Policy IT si intende per:

ACCESSO - Abilitazione all'esecuzione di applicazioni e/o al trattamento di dati.

ANTIVIRUS - Programma per elaboratore con la funzione di prevenire, rimuovere o limitare gli effetti provocati da virus informatici.

AUTENTICAZIONE INFORMATICA - L'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità.

BANCA DATI - Qualsiasi complesso e insieme di dati personali, ripartito in una o più unità dislocate in uno o più siti, organizzato secondo criteri e logiche tali da facilitarne il trattamento.

COMUNICAZIONE DEI DATI – L'atto di dare conoscenza dei dati personali a uno o più soggetti diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

CREDENZIALI DI AUTENTICAZIONE – Le informazioni ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica.

DIFFUSIONE DEI DATI - Il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

DOMINIO INFORMATICO - Insieme delle infrastrutture e delle risorse fisiche e logiche di proprietà della società destinate all'esercizio della sua attività d'impresa.

DOWNLOAD - Riproduzione sull'elaboratore elettronico, temporanea o permanente, totale o parziale, delle istruzioni che compongo un programma per elaboratore, ovvero dell'insieme di byte che compongono un file.

ELABORATORE ELETTRONICO (PERSONAL COMPUTER - PC) - Macchina elettronica digitale utilizzata da un incaricato del trattamento.

FILE - Unità logica di memorizzazione di qualsiasi tipo di contenuto o informazione.

FREEWARE - Programmi per elaboratore liberi di essere scaricati, utilizzati e distribuiti senza licenza d'uso.

LOG - Registrazione delle attività elaborative compiute da un'applicazione che permette di ricostruire le operazioni svolte da parte del codice identificativo dell'utente che ha operato.

PASSWORD – Equivalente ad una parola d'ordine, componente riservata di una credenziale di autenticazione associata ad una persona e a questa nota, costituita da una sequenza di caratteri alfanumerici o biometrici in forma elettronica.

POSTA ELETTRONICA - Messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o sul dispositivo ricevente, fino a che il destinatario non ne ha preso conoscenza.

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.

RETI DI COMUNICAZIONE ELETTRONICA - I sistemi di trasmissione, le apparecchiature di comunicazione e altre risorse che consentono di trasmettere i segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici (compresa Internet), le reti utilizzate per la diffusione di programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui sono utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato.

SCREEN SAVER - Applicazione che esegue la visualizzazione su monitor di una figura o motivo in movimento che, se abilitato, si attiva automaticamente dopo un determinato periodo di inutilizzo dell'elaboratore.

SHAREWARE - Programma per elaboratore che prevede l'utilizzo con funzionalità limitate a meno che non venga acquistata una licenza d'uso.

SICUREZZA INFORMATICA - Protezione del patrimonio informativo ed informatico da rilevazioni, modifiche o cancellazioni non autorizzate per cause accidentali o intenzionali e limitazione degli effetti causati dall'eventuale occorrenza di tali cause.

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.

STRUMENTI ELETTRONICI - Gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento di dati personali.

SUPPORTI DI MEMORIZZAZIONE – I supporti fisici (magnetici od ottici) destinati alla memorizzazione dei dati.

VIRUS INFORMATICO - Programma informatico avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento.

1. HARDWARE E SECURITY

Le apparecchiature informatiche, i programmi e tutte le varie funzionalità che CADIAI mette a disposizione dei suoi utenti devono essere utilizzate nel pieno rispetto delle norme indicate nella presente Policy IT al fine di evitare danni erariali, finanziari e di immagine della Cooperativa stessa. Tutto il personale interessato dalle disposizioni della presente Policy IT è tenuto a contattare il Responsabile Gestione Sistemi Informativi e Informatici prima di intraprendere qualsiasi attività non esplicitamente compresa nelle indicazioni che seguono, al fine di garantire che tali attività non siano in contrasto con gli standard di sicurezza informatica stabiliti dalla Cooperativa.

Le banche dati centrali e gli apparati di sicurezza informatica della rete aziendale sono installati nella Sala CED della sede della Cooperativa in via Bovi Campeggi in un locale videosorvegliato: ad accesso selezionato mediante un sistema a doppia chiave di accesso.

Negli uffici della Sede Centrale ad ogni operatore è assegnato un PC, un codice identificativo e una password sia per quanto riguarda l'accesso (login) che per quanto riguarda i programmi e le applicazioni (es. casella di posta) in esso istallate.

Le sedi esterne (Servizi in cui si erogano le attività della Cooperativa) sono dotate di PC affidati alla responsabilità dei Responsabili/Coordinatori che provvedono a definire in modo esplicito gli ambiti di accesso dei componenti del gruppo di lavoro sotto la propria responsabilità.

Nel caso di strumenti di lavoro condivisi tra più categorie di operatori (es. coordinatori ed educatori) è necessario creare ed accedere con profili diversi.

Gli strumenti di lavoro non dovranno essere condivisi con utenti o terzi.

I PC destinati agli utenti dovranno essere utilizzati sotto la stretta sorveglianza degli educatori e per le sole finalità dichiarate nei PEI/PAI.

Gli incaricati possono utilizzare strumenti di proprietà solo previa autorizzazione del Responsabile di Servizio, del Responsabile Gestione Sistemi Informativi e valutazione tecnica dell'Amministratore di Sistema nel rispetto delle prescrizioni definite della Cooperativa.

Per i dispositivi portatili (PC, smartphone, tablet, ecc.) sono previste le stesse regole di utilizzo previste dalla presente Policy IT.

Tali disposizioni si applicano anche nei confronti di responsabili esterni che utilizzano strumenti personali quali: medici, tecnici, ecc.

Il personal computer (fisso o mobile) ed i relativi programmi affidati a ciascun dipendente sono, come è noto, strumenti di lavoro, pertanto tali strumenti:

a) devono essere custoditi in modo appropriato (evitare di mangiare e bere sopra le apparecchiature, proteggerle da urti, polvere e liquidi, ecc.) e, in caso di accessi non autorizzati, atti dolosi, danni, furti, smarrimenti, malfunzionamenti, deve essere

tempestivamente avvisato il Responsabile di Servizio, il Responsabile Gestione Sistemi Informativi, il Referente Privacy e l'ufficio Amministrazione per la copertura assicurativa;

b) possono essere utilizzati solo per fini professionali (in relazione, ovviamente, alle mansioni assegnate) e non anche per scopi personali, tanto meno per scopi illeciti (ivi compresi: accessi non autorizzati, trattamento dati non consentiti o non conformi alla finalità della raccolta, ecc.);
   Una volta dismessi, i PC devono essere formattati da personale qualificato prima di procedere alla rottamazione o al loro riutilizzo; vanno pertanto consegnati in sede dopo avere cancellato i dati ivi contenuti. Detti accorgimenti sono estesi anche a telefonini, registratori, telecamere, macchine fotografiche, dispositivi magnetici (es. hard disk esterni, pen drive, schede SD), ecc.
   I supporti magnetici devono essere resi illeggibili prima di essere gettati o riciclati;
c) i PC in dotazione sono dotati di software per la crittografazione del contenuto del disco fisso; non vanno conservati comunque dati personali e sensibili sulle macchine, quando possibile.

Ai fini sopra esposti sono, quindi, da evitare atti o comportamenti contrastanti con le predette indicazioni come, ad esempio, quelli di seguito richiamati, a titolo indicativo:

a) non è ammessa la conservazione di dati personali e particolari di pertinenza non lavorativa sui dispositivi in uso; tali dati saranno considerati di proprietà personale e, pertanto, la Cooperativa ne disconosce qualsiasi titolarità e responsabilità;
b) non è consentita l'installazione di prodotti software se non regolarmente licenziati dai rispettivi produttori e senza la preventiva autorizzazione da parte del Responsabile Gestione Sistemi Informativi (vd. in proposito, gli obblighi imposti dal D.Lgs. 29 dicembre 1992, n. 518, sulla tutela giuridica del software e dalla L. 18 agosto 2000, n. 248, contenente nuove norme di tutela del diritto d'autore); tutto il software installato deve essere di proprietà e registrato a nome della Cooperativa e, nel rispetto della sopra citata legge (copyright), è fatto divieto ad ogni incaricato di installare, duplicare o utilizzare i vari software al di fuori di quanto consentito dagli accordi di licenza;
c) non è consentito l'utilizzo di piattaforme e software gratuiti per il trasferimento, la condivisione e/o l'archiviazione di dati senza l'autorizzazione dell'Amministratore di Sistema che a priori ne valuterà la sicurezza (es. Wetransfer, piattaforme/strumenti Google, ecc.);
d) non è consentito utilizzare software di proprietà personale ivi comprese le applicazioni regolarmente acquistate e registrate, programmi shareware e/o freeware, software scaricato da internet o proveniente da CD/DVD allegati a riviste e/o giornali o altro software posseduto a qualsiasi titolo;

e) è fatto divieto di creare o diffondere, intenzionalmente o per negligenza, programmi idonei a danneggiare il sistema informatico della Cooperativa, quali ad esempio virus, trojan horses, ecc.;

f) non è consentito, onde evitare il grave pericolo di introdurre virus informatici nonché l'alterazione della stabilità delle applicazioni dell'elaboratore, installare hardware, collegare dispositivi mobili personali (es. cellulari e tablet), e/o programmi in proprio: tutte le installazioni devono avvenire da parte dell'Ufficio Gestione Sistemi Informativi e ogni installazione non autorizzata sarà immediatamente rimossa. Ogni incaricato deve prestare la massima attenzione e cautela nell'effettuare il trattamento di dati memorizzati su supporti provenienti da ambienti operativi esterni al dominio aziendale, e in caso di necessità sottoporli all'Ufficio Gestione Sistemi Informativi che verificherà l'eventuale presenza di virus;

g) non è consentito utilizzare strumenti software e/o hardware atti ad intercettare, falsificare, memorizzare, comunicare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici (es. masterizzatori, modem, hard disk, driver, telecamere, macchine fotografiche, chiavi USB, ecc.). Non è consentita l'installazione su PC di mezzi di comunicazione propri. Sarà compito dell'Amministratore di Sistema sorvegliare e, eventualmente, procedere alla rimozione immediata di detti dispositivi;

h) non è consentito modificare le configurazioni impostate sul proprio PC e sulla strumentazione in uso o disattivare gli aggiornamenti automatici e l'autoprotezione dei sistemi;

i) non è consentito portare all'esterno dati personali e particolari senza l'autorizzazione del Responsabile di Servizio e senza previa cifratura. Non è consentito l'utilizzo di crittosistemi o di qualsiasi altro programma di sicurezza e/o crittografia non autorizzati esplicitamente dalla Cooperativa;

j) il computer non deve essere lasciato acceso oltre l'orario di utilizzo o in caso di assenze prolungate: 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;

k) non lasciare incustoditi computer portatili e altri dispositivi mobili (fotocamere digitali, smartphone, tablet) e conservarli con le necessarie precauzioni quando non utilizzati. In particolar modo si raccomanda di custodirli diligentemente anche di notte, durante gli spostamenti per evitare danni e sottrazioni (es. non lasciarli incustoditi in auto, stanze e atrii d'albergo, sale d'attesa, mezzi di trasporto, ecc.) nonché di rimuovere eventuali file elaborati prima della riconsegna;

l) è consentito, agli ospiti della sede centrale, di collegarsi alla rete wireless attraverso una rete "Guest".

In caso di necessità il Titolare del Trattamento coadiuvato dal Data Protection Officer ha facoltà di esaminare i dati trattati da ogni incaricato.

2. DISPOSITIVI MOBILI – NORME D'USO

I dispositivi mobili, smartphone, laptop e tablet, sono così configurati:

- crittografazione dei dati o di parte della memoria;
- password d'accesso e/o PIN;
- blocco schermo con PIN;
- software antivirus;
- programmi specifici per l'uso;
- servizio di cancellazione dei dati da remoto.

È cura dell'utente:

1) mantenere il codice PIN di adeguata complessità;
2) non disabilitare il blocco schermo;
3) verificare le impostazioni privacy e leggere le condizioni d'uso dei servizi durante le connessioni ad internet;
4) conservare con cura il codice IMEI che si trova sulla scatola del prodotto e che in caso di furto o smarrimento saranno utilizzati per bloccare a distanza l'accesso al dispositivo. L'Ufficio Gestione Sistemi Informativi, qualora lo riterrà necessario, provvederà inoltre alla cancellazione da remoto dei dati contenuti nel dispositivo;
5) scaricare regolarmente gli aggiornamenti software comprensivi di antivirus e di eventuali altri programmi di sicurezza;
6) non scaricare APP se non autorizzate dall'Amministratore di Sistema, anche se gratuite;
7) prima dell'utilizzo di APP verificare se viene chiesto l'accesso a contenuti presenti sul dispositivo (foto, contatti in rubrica, ecc.) e leggere le condizioni d'uso per evitare di dover pagare servizi non richiesti o esporre oltre misura informazioni di carattere personale o aziendale;
8) non installare software in violazione delle leggi sul diritto d'autore (L. 248/00) o sulla responsabilità amministrativa da reato (D.Lgs. 231/01);
9) non utilizzare connessioni (wifi e bluetooth) senza averne verificato l'attendibilità;
10) non utilizzare il cellulare privato in modalità fotocamera e telecamera per riprendere utenti, dipendenti, ecc.;
11) in caso di furto o smarrimento avvisare tempestivamente il Responsabile di Servizio il quale si occuperà a sua volta di informare l'Area e il Gruppo di lavoro Privacy prima di formalizzare eventuali denunce o querele;
12) non salvare sul dispositivo informazioni particolari (es. password, codici di accesso, dati bancari, ecc.);

13) non rispondere a messaggi provenienti da numeri sconosciuti: potrebbero contenere virus e link a servizi indesiderati a pagamento e programmi pericolosi per la privacy;
14) leggere attentamente ed adottare le medesime precauzioni illustrate nel paragrafo “Uso della rete internet e dei relativi servizi e Posta elettronica”;
15) non portare i dispositivi all’estero senza averlo comunicato ai responsabili ed avere avuto idonee autorizzazioni/coperture (ad esempio per il roaming);
16) non togliere la SIM dal dispositivo assegnato per spostarla su altri;
17) utilizzo limitato di chat/messaggeria istantanea (Whatsapp, Telegram, ecc.) avendo cura di non inviare messaggi, compreso allegati (es. foto e video), riguardanti dati personali di utenti e colleghi;

È vietato l’utilizzo di dispositivi (fotocamere, smartphone, tablet, ecc.) privati per scopi lavorativi.
L’impiego di computer personali (salvo i casi di smart working, vedasi paragrafo dedicato) è ammesso solo previa autorizzazione del Responsabile di Area-Servizio e opportune verifiche tecniche da parte dell’Amministratore di Sistema.

3. La Rete Aziendale (Dominio e applicazioni)

Il Responsabile Gestione Sistemi Informativi attiva o cessa le credenziali di accesso alla rete e alle banche dati con la collaborazione dell'Amministratore di Sistema, in base alle indicazioni ricevute dai Responsabili di Area/Settore, inoltre, mensilmente, rimuove tutti gli accessi assegnati agli utenti dimessi (dipendenti, liberi professionisti, terzi, ecc.).
Le credenziali ricevute non devono essere più utilizzate al decadimento o variazione della funzione specifica per le quali sono state assegnate (ad esempio in occasione di cambio servizio o mansione, cessazione del rapporto di lavoro).
Gli account utente vengono automaticamente disattivati quando non utilizzati per sei mesi salvo quelli creati dall'Amministratore di Sistema per scopi tecnici, da lui stesso gestiti. Le credenziali cessate, non devono essere riassegnate ad altri incaricati nemmeno in tempi diversi.
L'Amministratore di Sistema esamina periodicamente la rete al fine di verificare l'assenza di anomalie, malfunzionamenti, intrusioni, virus o altro.
Tutti gli endpoint della rete interna e delle sedi remote sono regolarmente sottoposti a processi di Vulnerability Assessment.

Il Responsabile Gestione Sistemi Informativi crea e aggiorna i profili di autorizzazione all'interno dei software gestionali o per i singoli incaricati o per classi omogenee di incarico.
Il Responsabile Gestione Sistemi Informativi mantiene costantemente aggiornato l'elenco delle credenziali di autorizzazione e la lista per classi omogenee di incarico con i relativi profili di autorizzazione riferiti ad ogni banca dati, ivi compreso l'elenco degli Amministratori di Sistema.
Il Responsabile Gestione Sistemi Informativi, coadiuvato dal Gruppo di Lavoro Privacy, monitora l'affidabilità e il rispetto delle misure di sicurezza dei fornitori di sistemi e dei prodotti forniti imposte dalla normativa vigente (Reg. UE 679/2016 art. 32) tramite la somministrazione annuale di questionari e/o Audit specifici.

Si riportano di seguito le indicazioni per un corretto utilizzo della rete aziendale.

1) Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo, essere utilizzate per scopi diversi. Pertanto, qualunque file che non sia legato all'attività lavorativa non può essere salvato, nemmeno per brevi periodi, in queste unità; la Cooperativa si riserva la facoltà di procedere alla rimozione di ogni file o applicazione che riterrà dannosi e/o essere pericolosi per la sicurezza del sistema ovvero acquisiti o installati in violazione del presente manuale di condotta.
2) La cartella di scambio dati (F:\DATI\LAVORO) deve essere unicamente utilizzata per la condivisione di documenti pesanti che non possono ad esempio essere inviati in posta

elettronica. Tali file devono essere rimossi immediatamente dopo il prelievo. È presente una procedura automatica per la rimozione periodica dei dati eventualmente rimasti all'interno della cartella. È VIETATO UTILIZZARE QUESTA CARTELLA PER IL PASSAGGIO, ANCHE TRANSITORIO, DI DATI PERSONALI compreso quelli SENSIBILI.

3) Per le necessità di condivisione di file e documenti aziendali al di fuori della sede è disponibile per gli utenti autorizzati un cloud aziendale (Qsync). L'accesso viene rilasciato dall'Ufficio Gestione Sistemi Informativi su richiesta dei Responsabili di Area/Settore e avviene tramite APP dedicata da PC o dispositivo mobile. In caso di accesso tramite interfaccia web è prevista la comunicazione crittografata SSL (https) e l'autenticazione a 2 fattori (Google Authenticator o invio codice via email). Su richiesta dei Responsabili di Area/Settore può essere messo a disposizione degli utenti aziendali un accesso remoto limitato a strumenti di elaborazione dati e spazio di archiviazione (telelavoro/smart working, ecc.) tramite connessione sicura VPN/SSL.
   Per il lavoro da remoto viene inoltre messo a disposizione un ulteriore strumento: TS-FARM che consente di collegarsi e avviare una connessione ad un server Cadiai presente nella rete interna ed accedere a dati e strumenti di lavoro come CUW2016, F:\Dati, Karthadoc, ecc. Per collegarsi a TS-FARM anche in questo caso è necessario instaurare una VPN (connessione diretta protetta) con la sede tramite Sonicwall Netextender o SMA, quindi l'accesso a TS-FARM crea una sessione di teleassistenza a un server remoto presente in sede, con la possibilità di aprire il desktop di questo server e operare direttamente su di esso, senza che rimangano dati di lavoro sul computer locale.
   Ogni utente dovrà essere opportunamente sensibilizzato sull'utilizzo dello strumento messo a disposizione secondo le linee guida aziendali definite (accesso, condivisione, rimozione degli archivi, ecc.).
4) Con regolare periodicità si deve provvedere alla pulizia degli archivi con cancellazione di file obsoleti ed inutili (prestando particolare attenzione alla duplicazione dei dati per evitare un'archiviazione ridondante) al fine di ottimizzare lo spazio disco disponibile e ridurre i rischi sui dati. Si raccomanda anche lo svuotamento costante del cestino sul proprio dispositivo.
5) Allo scopo di proteggere i dati da intrusioni esterne e di includerli nei salvataggi automatici, quando possibile viene richiesto al personale di salvare i propri documenti nelle cartelle di lavoro disponibili in rete (ad esempio in F:\DATI).

4. USO DELLA RETE INTERNET E DEI RELATIVI SERVIZI

Alla luce delle indicazioni fornite dal Garante per la Protezione dei Dati Personali, mediante il provvedimento generale del 01/03/2007 – *Linee guida per l'uso della posta elettronica e di internet sui luoghi di lavoro,* l'Ufficio Gestione Sistemi Informativi ha implementato le seguenti misure di sicurezza a protezione della rete aziendale:

- prevenzione di intrusioni con scansione antivirus (funzionalità IPS);
- rilevamento e segnalazione di tentativi di attacco;
- notifica di vulnerabilità riscontrate e ricezione di aggiornamenti correttivi;
- rilevamento e blocco di programmi IM, P2P;
- filtraggio dell'accesso ai siti non attinenti l'attività lavorativa e che possono esporre l'azienda a rischio di contagio (Content Filtering Service).

L'Amministratore di Sistema ai fini della sicurezza della rete e dei sistemi aziendali effettua costanti e periodici controlli sui dati di traffico internet. È compito dell'Amministratore di Sistema mettere in atto idonee azioni al fine di prevenire e gestire incidenti informatici.

Al fine di prevenire il danno che può causare l'utilizzo scorretto di internet, ad ogni utente è richiesto un comportamento rispettoso dell'etica e delle norme di buon uso dei servizi di rete. In particolar modo si specifica che:

1) non è consentito l'utilizzo di internet per scopi vietati dalla legislazione vigente. L'utente è direttamente responsabile, civilmente e penalmente, per l'uso fatto del servizio di internet. La responsabilità si estende anche alla violazione degli accessi protetti, del copyright e delle licenze d'uso;
2) non è autorizzato l'utilizzo per scopi di lucro e per qualsiasi attività economica non riconducibile alle finalità lavorative;
3) non è consentita l'effettuazione di ogni genere di transazione finanziaria come operazioni di remote banking, acquisti on-line e simili, salvo casi direttamente autorizzati dal Presidente e dal Responsabile Amministrativo e con il rispetto delle normali procedure d'acquisto;
4) qualora si sia autorizzati ad eseguire pagamenti on line, diffidare di offerte economiche, sconti, vantaggi, promozioni e/o regali provenienti da siti sconosciuti;
5) non inserire dati bancari in siti non noti o siti in cui non vengono rispettate le procedure di sicurezza standard per le transazioni on line (protocolli https);
6) non navigare in siti non attinenti allo svolgimento delle mansioni assegnate, in particolare siti dai quali si possono desumere informazioni personali di natura religiosa, sindacale, politica e sanitaria;
7) non accedere a siti mediante azione inibente dei filtri, sabotando, superando o tentando di superare, disabilitando i sistemi adottati dalla Cooperativa per bloccare accessi

ritenuti non conformi all'attività lavorativa o dannosi per i sistemi, non usare sistemi che realizzino tale fine;

8) fare attenzione ai falsi siti, ad esempio quelli il cui nome non corrisponde al nome dell'azienda che dovrebbe gestirlo;
9) non scaricare e/o condividere di file tipo MP3, AVI, MPG, MOV e/o altri tipi di files o programmi per la fruizione o la condivisione (P2P) di contenuto audio/video non legati all'uso professionale;
10) non eseguire download di software gratuiti (freeware) e shareware se non espressamente autorizzati dal Responsabile Gestione Sistemi Informativi;
11) non registrarsi su social network con account aziendali o legati ai servizi della Cooperativa se non espressamente autorizzati dalla Direzione;
12) non partecipare, per motivi non professionali, a dibattiti, forum, blog, concorsi, aste on line, catene telematiche, mailing-list, chat line, petizioni, bacheche elettroniche e guestbook anche utilizzando pseudonimi (nicknames);
13) non pubblicare dati personali di clienti, fornitori, dipendenti o contenuti aziendali su social network e piattaforme web (nemmeno ritenute attendibili e protette) se non espressamente autorizzati dalla Direzione;
14) non pubblicare mai dati sensibili su qualsiasi piattaforma online;
15) come precisato al paragrafo 8.1. è necessario acquisire le relative liberatorie per procedere alla pubblicazione di foto e/o video ed accertarsi che la foto o la ripresa rientri all'interno di un progetto o di un'attività autorizzata;
16) scegliere con cautela le connessioni wifi gratuite a cui collegarsi quando si è in viaggio: potrebbero non essere adeguatamente protette ed esporre PC, smartphone e tablet ad intrusioni esterne da parte di malintenzionati;
17) prestare attenzione all'apertura di link o allegati a messaggi di posta elettronica in quanto potrebbero contenere virus, malware (cioè programmi dannosi), software spia, phishing (cioè frode finalizzata all'acquisizione, per scopi illegali, di dati riservati dell'utente), ecc.

5. POSTA ELETTRONICA

La posta elettronica è uno strumento di lavoro e si richiede un suo utilizzo corretto e professionale attinente allo svolgimento delle mansioni assegnate ed in particolare si precisa che:

1) la posta elettronica diretta all'esterno della rete informatica aziendale può essere intercettata da estranei, dunque non deve essere usata per inviare documenti di lavoro "strettamente riservati" o "particolari". In caso di scambio occasionale di dati è consentito l'utilizzo di allegati compressi (zip) protetti da password, quest'ultima da comunicarsi con altro mezzo. Salvo specifiche deroghe autorizzate espressamente qualora la corrispondenza sia frequente (con lo stesso interlocutore) è necessario contattare l'Amministratore di Sistema per predisporre una modalità diversa di comunicazione (es. utilizzando il cloud aziendale);
2) ogni comunicazione da inviarsi che abbia contenuti rilevanti (impegni contrattuali o precontrattuali per CADIAI, documenti da considerarsi riservati, ecc.), deve essere contraddistinta dalla dicitura "Confidenziale" o "Riservato";
3) per le comunicazioni ufficiali si chiede di utilizzare gli strumenti tradizionali (fax, posta raccomandata) o PEC anziché email con ricevuta di ritorno in quanto non aventi valore legale;
4) l'email istituzionale del servizio è ad uso del Responsabile di Servizio, pertanto il suo accesso e la sua consultazione sono riservati in via esclusiva a lui. Il Responsabile di Servizio ha comunque facoltà di nominare un fiduciario che potrà accedere alla casella in caso di sua assenza;
5) confrontarsi sempre con l'Ufficio Privacy prima di eseguire invii di email di tipo commerciale al fine di verificarne la liceità (ad esempio se si è in possesso del consenso dei destinatari, se si ha già in essere un rapporto per un prodotto o servizio analogo già venduto, se è presente in calce al messaggio il diritto di recesso, ecc.);
6) non aprire o rispondere a messaggi di posta elettronica il cui mittente sia sconosciuto o sospetto, ma procedere alla loro rimozione o contattare l'Ufficio Gestione Sistemi Informativi;
7) non cliccare sui link contenuti nelle email se non si è certi dell'affidabilità del sito a cui si è rimandati. In questo caso una semplice precauzione è quella di passare il mouse sul link stesso **senza cliccarlo** e verificare, nel riquadro che apparirà, l'URL (cioè l'indirizzo web) reale al quale si potrebbe essere indirizzati. Questi link potrebbero essere collegati a sistemi che tentano truffe telematiche e furti di identità, ma anche aprire la strada a software spia o virus informatici;

8) non rispondere allo spam: la risposta può consentire allo spammer di stabilire che il tuo indirizzo email è valido e attivo, continuare ad inviarti Spam, vendere il tuo indirizzo verificato a terzi, sfruttare il contatto creato per portare avanti tentativi di truffa;
9) qualora le comunicazioni pubblicitarie o altro tipo di richieste (es. newsletter, ecc.) risultassero ad un certo punto indesiderate si ha il diritto di opporsi al trattamento dei dati utilizzando le procedure online per la cancellazione, contenute nel corpo del messaggio;
10) fare attenzione qualora si intenda inviare una email a diversi destinatari a non rendere visibili gli indirizzi dei vari contatti, usando la funzione CCN (destinatario in copia conoscenza nascosta);
11) quando ci si appresta ad inviare una email prestare la massima attenzione alla compilazione automatica durante la digitazione dell'indirizzo, spesso il campo viene compilato in automatico (con un indirizzo con gli stessi caratteri digitati inizialmente presente in memoria) e si corre il rischio di sbagliare il destinatario;
12) non aprire allegati di tipo eseguibile (in particolare file con estensione .exe, .scr, .pif, .bat, .cmd, ecc.) e, se non si è sicuri del mittente, evitare di scaricare anche le immagini eventualmente contenute nel corpo del messaggio in quanto potrebbero contenere virus;
13) non utilizzare email personali su PC connessi alla rete aziendale;
14) cancellare immediatamente il messaggio in caso di ricezione anche accidentale di email personali sulla mail aziendale al fine di evitare la memorizzazione e il salvataggio nei sistemi aziendali;
15) verificare (inviando una email a sé stessi) che in calce ai messaggi compaia la declaratoria privacy che ne identifica la titolarità e ne vieta l'uso improprio;
16) non inviare messaggi di posta elettronica, anche all'interno della rete aziendale, che abbiano contenuti contrari a norme di legge ed a norme di tutela dell'ordine pubblico, rilevanti ai fini di una fattispecie di reato o che siano in qualche modo offensivi dei principi di dignità personale, di libertà religiosa, di libertà sessuale o di manifestazione del pensiero, anche politico a contenuto violento, sessuale o discriminatori dell'origine etnica, del colore della pelle, della fede religiosa, dell'età, del sesso, della cittadinanza, dello stato civile, degli handicap; in caso di ricezione di tali messaggi si è pregati di eliminarli immediatamente;
17) mantenere in ordine la casella di posta cancellando documenti inutili o superati (la posta è assistita dalle stesse garanzie della corrispondenza e pertanto va rimossa seguendo le stesse indicazioni riportate nelle Procedure aziendali) e soprattutto allegati ingombranti: al raggiungimento del limite di occupazione assegnato la stessa si bloccherà impedendo la ricezione di nuovi messaggi;

18) impostare un messaggio di “fuori sede” sulla casella di posta in caso di assenza programmata ed indicare eventualmente nel messaggio il nominativo del collega d’ufficio o preposto per la sostituzione, senza “dirottare” le email in automatico sulla sua casella.

La casella di posta, in caso di dimissioni o, eventualmente, di cambio mansione, viene chiusa dopo pochi giorni inserendo temporaneamente un messaggio automatico volto ad informare della variazione e a fornire indirizzi alternativi riferiti all’attività professionale di CADIAI. I contenuti ritenuti di proprietà aziendale, possono essere salvati altrove all’occorrenza o eliminati prima della chiusura della casella di posta.

6. BACKUP – SUPPORTI DI MEMORIZZAZIONE

FREQUENZA E VERIFICA

Sui server della sede il salvataggio dei dati avviene in automatico ogni 24 ore (generalmente la notte) su dispositivi Storage di rete (NAS) con volumi crittografati. Al termine del salvataggio il server invia un messaggio di avvenuta esecuzione nella posta elettronica al Responsabile Gestione Sistemi Informativi e dell'Amministratore di Sistema, i quali dovranno accertarsi del buon esito dell'operazione.

Le sedi periferiche più complesse (con un maggior numero di computer), sono dotate di Storage di rete (NAS), mentre nei restanti casi (strutture e servizi di piccole dimensioni e/o figure tecniche quali psicologi e pedagogisti) sono dotate di dispositivi di memorizzazione esterni crittografati (HDD USB crittografati).

Nel primo caso ogni computer è configurato in modo da effettuare automaticamente e quotidianamente una copia dei dati su di esso presenti, senza alcun intervento manuale.

Nel secondo caso il backup viene invece effettuato manualmente, previo collegamento al computer dell'hard disk esterno: tale operazione innescherà automaticamente la copia dei dati sull'hard disk stesso. Il backup va eseguito regolarmente e almeno con cadenza settimanale.

In entrambi i casi il Coordinatore di Servizio o l'Assegnatario del dispositivo di backup verifica il corretto svolgimento delle operazioni di salvataggio dei dati visualizzando l'interfaccia del programma utilizzato (Veeam Backup) e informando l'Ufficio Gestione Sistemi Informativi qualora venissero riscontrate delle anomalie.

I tecnici monitoreranno periodicamente la funzionalità dei backup durante gli audit e ad ogni intervento di manutenzione sul PC.

I dispositivi mobili (quali fotocamere, smartphone, tablet, ecc.) vanno regolarmente svuotati da foto e dai dati contenuti, salvandoli negli appositi supporti di back up.

DISPOSITIVI: USO CORRETTO, CUSTODIA, RIUTILIZZO, MANUTENZIONI

I dispositivi per i salvataggi sono forniti da CADIAI al fine di garantirne l'ottima qualità e non comprometterne l'efficacia. È ammesso solo l'utilizzo di chiavette crittografate.

Non è consentito effettuare backup aggiuntivi su dispositivi diversi da quelli forniti.

Furti e danni vanno tempestivamente denunciati all'Area la quale informa l'Ufficio Privacy.

I dispositivi di backup devono essere riposti in luogo protetto (chiuso a chiave), in alto (per evitare rischi di allagamento), ecc. I dispositivi magnetici non devono essere mai sottoposti a fonti di calore, fonti magnetiche (es. casse acustiche), rischio di contatto con sostanze nocive e liquidi (anche accidentalmente es. Coca Cola, ecc.).

Tutti i supporti di salvataggio caduti in disuso devono essere sempre resi all'Ufficio Gestione Sistemi Informativi al fine di renderne illeggibile il contenuto.

7. Restore – Disaster Recovery

In caso di file persi o danneggiati l'incaricato deve avvertire tempestivamente l'Ufficio Gestione Sistemi Informativi che si occuperà, ove possibile, del ripristino dei dati.

Il Disaster Recovery aziendale prevede il salvataggio remoto su sede esterna dei dati presenti sui server tramite replica delle macchine virtuali presenti nell'ambiente e posizionati su Storage esterno con volumi crittografati.

8. Credenziali di autenticazione

FREQUENZA

Le credenziali di accesso alla rete aziendale hanno durata bimestrale: alla scadenza il sistema richiede il cambio password garantendo la riservatezza e l'autonomia dell'operatore (Ex DPR 318/99 – Art. 2 – Comma 1a).

La password deve inoltre essere sostituita tempestivamente all'occorrenza ogni volta che abbia perduto la propria riservatezza.

Nei computer delle sedi remote, e/o comunque non direttamente collegati al dominio aziendale, viene impostata localmente una policy che impone il cambio periodico delle credenziali ogni due mesi.

Qualora il cambio password non venga richiesto, l'operatore è tenuto a segnalarlo all'Ufficio Gestione Sistemi Informativi per le verifiche del caso.

MODALITÁ DI ESECUZIONE E CUSTODIA

- Ogni incaricato deve verificare che il PC in dotazione sia fornito di password e cambiarla al primo accesso.
- La password, come da definizione dell'Ex DPR 318, "*non deve essere banale (ad esempio la ripetizione dello USER ID) e non deve apparire in chiaro quando digitata*" e seguire le regole:
  - essere lunga almeno 8 caratteri;
  - contenere numeri e lettere;
  - contenere caratteri speciali (es. segni di punteggiatura, ecc.);
  - contenere almeno una lettera maiuscola ed una minuscola;
  - non ripetere la stessa stringa durante gli aggiornamenti successivi;
  - non trascriverla e lasciarla in posti facilmente raggiungibili da altri (es. sotto la tastiera);
  - non divulgarla;

- non rivelare le proprie credenziali per l'accesso a servizi quali posta elettronica, rete, banche dati, ecc.;
- non utilizzare il nome utente e la password di altri utenti;
- custodirla con diligenza e adottare ogni necessaria cautela per assicurarne la segretezza e l'uso esclusivo.

- In caso di accesso al computer in assenza dell'utente per motivi straordinari, l'Amministratore di Sistema su richiesta del Responsabile Gestione Sistemi Informativi reimposta le credenziali di accesso.
  Il Responsabile, dopo l'eventuale attivazione straordinaria del PC, vigila sul suo utilizzo e ha cura di spegnerlo cambiando la password con una provvisoria. L'interessato viene tempestivamente avvisato dell'intervento effettuato ed invitato ad inserire un nuovo codice identificativo quanto prima.
- L'incaricato può chiedere in caso di assenza che l'accesso al suo PC sia effettuato alla presenza di un collega di fiducia dandone preventiva comunicazione al Responsabile Gestione Sistemi Informativi.
- In sede le credenziali di accesso a dati strategici (home banking), le chiavi e altri dispositivi di autenticazione (smart card, business key), carte di credito, devono essere conservati in cassaforte o in altri luoghi sicuri;
- Le password dell'Amministratore di Sistema sono raccolte e depositate seguendo le istruzioni dell'apposita procedura.

PROTEZIONI E VERIFICHE

L'account utente si blocca ed è necessario l'intervento dell'Amministratore di Sistema:

- dopo 8 tentativi di accesso digitando erroneamente la propria password;
- se si è dimenticata la password.

L'Amministratore di Sistema è abilitato alla sola sostituzione delle credenziali e non alla lettura della password attuale.

Gli account non utilizzati o riferiti a personale dimesso vengono tempestivamente disattivati.

ALTRE INDICAZIONI

- Ad ogni utente è richiesto di bloccare il proprio computer ogni volta che è prevista un'assenza prolungata dalla postazione di lavoro.
- È data indicazione ad ogni incaricato di verificare che sul proprio dispositivo sia inserito lo screensaver con password (sui PC collegati alla rete aziendale è automatico dopo 15 minuti di inutilizzo) e di impostarlo con le istruzioni impartite o chiederne l'attivazione all'Ufficio Gestione Sistemi Informativi in caso di difficoltà.
- È consentita l'attivazione di password al BIOS solo previo accordo con l'Amministratore di Sistema.
- È assolutamente proibito entrare nella rete e nei programmi con credenziali diverse dalle proprie, nonché condividerle con altri.

- Ogni banca dati deve essere protetta mediante richiesta di credenziali d'accesso.
- E' vietata la rimozione delle credenziali dalle strumentazioni in uso.

9. PROTEZIONE ANTIVIRUS

Nonostante il sistema informatico di CADIAI sia protetto da software antivirus aggiornato quotidianamente e da dispositivi hardware di filtraggio, ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco da virus ed altri software dannosi.

La posta elettronica e la navigazione su internet sono sottoposte a controllo dagli apparati di rete.

Nel caso in cui venga rilevato un malware o virus, a seconda del livello di rilevamento, può essere inviato un alert riepilogativo all'utente finale e l'eventuale allegato posizionato in area di quarantena.

CADIAI ha dotato la sede e la maggior parte dei servizi di un software che inibisce la navigazione su siti non pertinenti l'attività lavorativa.

MODALITÁ DI FUNZIONAMENTO

L'**antivirus** utilizzato è Avast Business Security ed è installato su ogni client al fine di proteggere i dati in esso contenuti. Gli aggiornamenti vengono scaricati da Internet automaticamente non appena il fornitore li mette a disposizione online.

Il programma, una volta identificato un virus, lo rende immediatamente inattivo ed invia un messaggio di avvertimento all'utilizzatore del PC.

L'Amministratore di Sistema dispone di una console di monitoraggio e di gestione, per la visualizzazione e l'analisi degli attacchi subiti.

È vietato agli incaricati apportare modifiche di configurazione al software antivirus o disattivarlo.

INDICAZIONI

In caso di sospetta infezione da virus si deve:

- sospendere ogni elaborazione in corso senza spegnere il computer;
- staccare il PC dalla presa di rete;
- avvertire tempestivamente l'Ufficio Gestione Sistemi Informativi per l'immunizzazione;
- non inviare messaggi di posta elettronica;
- non passare file ad altri anche tramite l'utilizzo di supporti magnetici (es. pen drive, ecc.).

CONTROLLI

Periodicamente l'Amministratore di Sistema esamina la rete al fine di verificare l'assenza di anomalie, malfunzionamenti, intrusioni, virus o altro e formula nuove strategie per prevenire gli attacchi.

10. Siti Web

Non è consentito aprire o modificare siti web, blog, pagine o post su social network intestati o per conto della Cooperativa e/o ai Servizi senza aver prima informato l'Ufficio Privacy e l'Ufficio Comunicazione.

L'accesso ai siti web aziendali, alle pagine istituzionali e alle aree riservate dedicate al personale, è protetto mediante protocollo crittografato SSL (HTTPS) e password.

11. Videosorveglianza

L'installazione di sistemi di videosorveglianza prevede iter autorizzativi complessi affinché siano conformi alla disciplina vigente (L. n.300/1970, Regolamento UE 2016/679, D.Lgs n.196/2003 così come modificato dal D.Lgs 101/2018, Provv. Aut. Garante in tema di videosorveglianza 08/04/2010).

Qualora si ravvisi la necessità di modificare, attivare un nuovo impianto, o in caso di subentro nella gestione di servizi dotati di impianti di videosorveglianza installati da altri enti/organizzazioni, compete all'Ufficio Privacy, in collaborazione con il DPO ed eventuali altre funzioni aziendali coinvolte, effettuare le opportune valutazioni ed avviare l'iter di autorizzazione e/o di messa a norma. Non è pertanto consentita l'operatività di impianti di videosorveglianza che non abbiano seguito il suddetto iter.

12. Geolocalizzazione

L'adozione di apparecchiature o sistemi di geolocalizzazione (GPS) comportano adempimenti specifici per la tutela della privacy degli interessati; occorre pertanto preventivamente attivare l'Ufficio Privacy e le eventuali altre funzioni aziendali coinvolte per la verifica della liceità del trattamento e per la regolarizzazione a norma di legge.

13. Cloud Computing

Il Responsabile Gestione Sistemi Informativi, qualora i dati siano esternalizzati in infrastrutture cloud computing (tecnologie e modalità di fruizione di servizi informatici che favoriscono l'utilizzo e l'erogazione di software nonché la possibilità di conservare e di elaborare grandi quantità di informazioni via internet utilizzando sistemi del fornitore) valuta i rischi e le possibili conseguenze (sicurezza, ruoli e responsabilità, disponibilità del servizio e piano di emergenza, recupero dati, confidenzialità, collocazione dei server, migrazione, assicurazione sul danno, ecc.).
Si accerta che siano adottate le cautele necessarie: nomina il fornitore quale Responsabile esterno del trattamento, verifica e negozia la presenza di adeguate clausole contrattuali (sicurezza, ruoli e responsabilità, portabilità, accessibilità, controllo, assicurazione sul danno, ecc.).
Le banche dati salvate nei servizi Cloud non vengono comunque trasferite fuori dal territorio dell'Unione Europea.

14. Espletamento Attività Con Strumenti Propri

La presente sezione si applica ai soli lavoratori che svolgono la propria attività con strumenti propri e in luoghi diversi dalle sedi aziendali purché autorizzati dal proprio responsabile a prescindere che sia instaurato un rapporto di smart working per il quale si rinvia alla sezione seguente.
Il lavoratore è tenuto a:

- NON effettuare stampe e NON custodire copie cartacee dei documenti trattati; NON effettuare estrapolazioni dai gestionali se non strettamente necessarie ed eliminarle in modo sicuro;
- NON effettuare copie di salvataggio (backup) dei dati trattati su supporti personali (PC, hard disk, chiavette USB, ecc.), salvo espressa autorizzazione e comunque utilizzando i supporti forniti dalla Cooperativa;
- provvedere a caricare (c.d. upload) le informazioni trattate sul cloud aziendale o sulla piattaforma messa a disposizione per l'espletamento del proprio lavoro;
- assicurarsi che durante la sessione di lavoro nessun soggetto non autorizzato (es. familiari, conviventi, amici, ecc.) possano accedere alle informazioni trattate (es. osservando il monitor, ecc.);
- assicurarsi che gli strumenti utilizzati per l'attività lavorativa siano adeguatamente protetti (es. password, antivirus, firewall, ecc.);

- NON eseguire screenshot del monitor durante una sessione di lavoro, o scattare fotografie o realizzare video;
- nel caso in cui sia necessario salvare in locale un documento al fine di trasmetterlo via email o caricarlo sulla pertinente piattaforma è obbligatorio proteggerlo con una password di adeguata complessità e successivamente eliminarlo;
- ogni variazione sostanziale deve essere caricata e salvata per non perdere le modifiche.

15. SMART WORKING

Nello svolgimento dell'attività lavorativa, oltre a quanto previsto nelle sezioni precedenti, lo smart worker (lavoratore agile) deve osservare quanto segue:

OBBLIGHI PER IL DIPENDENTE

- Lo svolgimento della prestazione lavorativa dovrà avvenire secondo le direttive e nel rispetto delle attività assegnate dal proprio responsabile.
- Nello svolgimento della prestazione lavorativa, il comportamento dello smart worker dovrà essere improntato a principi di buona fede e di correttezza.
- Durante le giornate di "smart working", salvo il periodo di pausa, di riposo e di disconnessione, nell'ambito del normale orario di lavoro, lo smart worker dovrà rendersi reperibile e contattabile tramite gli strumenti aziendali messi a sua disposizione. In caso di riunione programmata dalla Cooperativa, il dipendente deve rendersi disponibile a partecipare di persona o da remoto, per il tempo necessario per lo svolgimento della riunione stessa. In caso di esigenze organizzative, a richiesta del responsabile, il dipendente dovrà presentarsi presso la sede di lavoro.

GESTIONE DEI DATI E DELLE INFORMAZIONI

- Ogni dipendente dovrà esercitare la prestazione al di fuori delle sedi aziendali e quindi in "smart working" scegliendo un luogo idoneo, che consenta il pieno esercizio della propria attività lavorativa nel rispetto della normativa interna e della legislazione vigente in tema di protezione dati (Privacy) e di riservatezza delle informazioni/documenti trattati.
- Lo smart worker è responsabile della riservatezza dei dati e delle informazioni trattate.
- Nello specifico non sarà possibile portare fuori dalle sedi di lavoro documenti in formato cartaceo, salvo espressa e motivata autorizzazione.
- Il lavoratore che effettua la propria prestazione in "smart working" è tenuto alla più assoluta riservatezza sui dati e sulle informazioni aziendali in suo possesso e/o disponibili su software/sistemi aziendali e/o su documenti cartacei.

DOTAZIONI INFORMATICHE

- I dipendenti in smart working utilizzeranno l'attrezzatura tecnologica fornita dalla Cooperativa (PC aziendale, smartphone aziendale, zoom, ecc.) o gli strumenti propri secondo le indicazioni fornite anche nei precedenti paragrafi.
- Il dipendente si impegna a custodire con la massima cura e mantenere integra la strumentazione che sarà fornita, in modo da evitarne il danneggiamento e lo smarrimento e utilizzarla in conformità con le istruzioni ricevute nel rispetto di quanto previsto dalle policy e dei regolamenti aziendali.
- Condizione necessaria per l'ammissione al progetto di "smart working" è il disporre di una connessione internet ADSL privata, o similare, già attiva e performante.
- Al fine di fruire dei sistemi aziendali non pubblici (es. gestionali aziendali, ecc.) che possono essere raggiunti solo in rete aziendale il dipendente dovrà utilizzare il collegamento VPN messo a disposizione dalla Cooperativa.
- Il dipendente ha l'obbligo di utilizzare e custodire gli strumenti di lavoro affidatigli nel rispetto delle norme in materia di salute e sicurezza del lavoro e a adottare le necessarie precauzioni affinché terzi, anche se familiari, non possano accedere agli strumenti di lavoro.
- Per gli aspetti non previsti dalla presente policy si fa riferimento alla regolamentazione interna specifica in merito al lavoro agile *"Informativa sulla salute e sicurezza nel lavoro agile".*

16. MONITORAGGIO

CADIAI può monitorare l'utilizzo delle proprie risorse informatiche in conformità con questa policy e nel rispetto della disciplina giuslavoristica. Nell'ambito del corretto funzionamento e della protezione degli interessi di CADIAI, la stessa attraverso l'Amministratore di Sistema esaminerà la rete al fine di verificare l'assenza di anomalie, malfunzionamenti, intrusioni, virus o altro e potrà accedere e rivedere tutti i materiali che gli utenti creano, memorizzano, inviano o ricevono sulle risorse informatiche di CADIAI.
CADIAI esclude controlli prolungati, costanti o indiscriminati.

In caso di anomalie, su segnalazione dell'Amministratore di Sistema CADIAI procederà con avvisi generalizzati diretti ai dipendenti del servizio/ufficio in cui è stata rilevata l'anomalia, nei quali si evidenzierà l'utilizzo irregolare degli strumenti aziendali e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati ed alle istruzioni impartite.

Controlli su base individuale potranno essere compiuti solo in caso di successive ulteriori anomalie o in caso di grave inadempienza capace di mettere a rischio la sicurezza informatica di CADIAI e/o la riservatezza, integrità e disponibilità dei dati personali trattati.
In caso di richiesta di assistenza tecnica il personale addetto potrà intervenire da remoto sui PC con il consenso dell'incaricato a cui rimarrà la visione delle operazioni effettuate durante l'intervento.

17. Sanzioni disciplinari per mancata osservanza della Policy IT

Il mancato rispetto di quanto disposto dalla presente Policy IT costituisce infrazione disciplinare ed è perseguibile secondo quanto prescritto dalla Contrattazione Collettiva di settore.

CADIAI
COOPERATIVA SOCIALE

Eventuali segnalazioni al possono essere inviate a:

CADIAI – Ufficio Privacy
Via Bovi Campeggi 2/4 E – 40131 – Bologna
privacy@cadiai.it

Appendice 4 – Procedura gestione risorse umane

INDICE

Revisione	Data	Motivo	Verifica	Approvazione
0	30/04/2003	Nuova edizione		
1	24/10/2007	Modifica di alcune prassi		
2	15/09/2009	Introduzione di nuove prassi		
3	16/09/2010	Introduzione di nuove prassi		
4	1/06/2011	Introduzione di nuove prassi		
5	31/10/2013	Modifiche organizzative		
6	31/05/2014	Modifiche organizzative		
7	16/09/2015	Modifiche organizzative		
8	01/12/2016	Introduzione di alcune specifiche		
9	11/03/2019	Modifiche organizzative e di alcune prassi		
10	31/10/2019	Aggiornamenti organizzativi		
11	25/11/2020	Aggiornamenti organizzativi		
12	21/11/2023	Aggiornamenti organizzativi e introduzione nuove prassi		

1. SCOPO

Scopo della procedura è la definizione delle modalità attraverso le quali la Direzione di CADIAI provvede al reclutamento e alla gestione del personale interno alla Cooperativa, garantendone la valorizzazione delle competenze, la partecipazione ai processi organizzativi, la tutela della salute e della sicurezza e stabilendo obiettivi di sviluppo e qualificazione in tutte le tipologie di attività aziendali.

2. APPLICABILITÀ

Oggetto della procedura sono tutte quelle attività che consentono di individuare le necessarie risorse umane, inserirle in tutte le aree, accrescerne la motivazione, migliorarne la comunicazione e le prestazioni.
In particolare, la procedura è utilizzata al fine di garantire il corretto svolgimento delle seguenti attività:

1. Pianificazione organizzativa del personale;
2. Selezione;
3. Assunzione;
4. Inserimento (affiancamento e addestramento);
5. Definizione dei percorsi di carriera;
6. Valutazione della motivazione e della soddisfazione;
7. Valutazione dello stress da lavoro correlato e/o dell'eventuale grado di burn-out;
8. Valutazione delle prestazioni svolte;
9. Gestione delle relazioni sindacali;
10. Dimissione;
11. La rilevazione dei dati sulle presenze del personale, utilizzato ai fini del Controllo di Gestione e della definizione del Fabbisogno di personale per i Servizi Operativi;
12. L'elaborazione di dati e statistiche sul personale da sottoporre alla valutazione del Consiglio di Amministrazione e della Direzione.

Le aree coinvolte nelle attività relative alla gestione delle risorse umane sono le seguenti:

- Consiglio di Amministrazione
- Direzione
- Segreteria Generale
- Area Risorse Umane
- Area Amministrazione Generale
- Servizio Prevenzione e Protezione
- Responsabili di Area/Settore
- Coordinatrici/tori dei Servizi
- Organismo di Vigilanza
- Comitato per la Responsabilità Sociale
- Comitato per la Salute e la Sicurezza
- Responsabile Politiche Pari Opportunità
- Comitato per le Pari Opportunità
- Area Sistema di Gestione (Unità Gestione Sistemi Informativi; Unità Gestione Privacy)

3. RIFERIMENTI

3.1 DOCUMENTAZIONE INTERNA APPLICABILE

- Manuale del Sistema di Gestione

- Regolamento Interno
- Politiche retributive
- Codice Etico
- Profili Professionali e Funzionali in CADIAI
- Cartellina per neo assunti
- Fascicolo dell'operatrice/tore
- Istruzione Operativa "Mobilità - Ricollocazione del personale"
- Istruzione Operativa "Assunzione, gestione e dimissione del personale"
- "Domanda di Lavoro" (on line in software Zucchetti)
- "Scheda colloquio selezione" (on line in software Zucchetti)
- "Elementi necessari per l'assunzione"
- "Pianificazione dell'affiancamento/inserimento in servizio"
- Pianificazione dell'affiancamento/inserimento in ruolo
- "Questionario per l'autovalutazione delle competenze e la rilevazione del fabbisogno formativo"
- "Foglio Presenze"
- "Questionario di soddisfazione del personale"
- "Questionario sulla salute e sicurezza sul lavoro"
- "Richiesta di mobilità"
- "Dimissioni da socio"
- Documenti di programmazione annuale di aree/settori e dei servizi di staff
- "Scheda di progetto"
- Modulo "Richiesta accessi informatici aziendali"
- Documentazione privacy (es. informative, consensi, nomine, domande di lavoro, …)
- Regolamenti aziendali (opuscoli) in tema di privacy "I principi generali del Regolamento UE 679/2016" e "Il Regolamento di Cadiai: norme comportamentali e policy IT"
- Opuscolo informativo "Salute e sicurezza sul lavoro"

4. DESCRIZIONE DELLE ATTIVITÀ

4.1 PIANIFICAZIONE ORGANIZZATIVA DEL PERSONALE

Le/i Responsabili di Area produttiva/Settore coadiuvate/i dalle/i Responsabili di produzione e le/i Responsabili delle Aree di Staff pianificano annualmente la quantità e la tipologia di personale necessarie per consentire il corretto svolgimento delle attività dei servizi. Tale pianificazione, in linea di massima, prescinde dal genere delle persone, a meno che riguardo a quest'ultimo non ci siano specifiche esigenze riferite all'utenza dei servizi.

La pianificazione viene svolta sulla base dei seguenti elementi:

- dati provenienti dal Controllo di Gestione;
- dati e statistiche provenienti dall'Area Risorse Umane;
- numero di dimissioni presentate;
- piano ferie di ciascun servizio;
- valutazione dei bisogni complessivi e specifici dei servizi;
- richieste contingenti e/o contrattuali ad opera della committenza.

Una volta definito il numero ed il tipo di persone necessarie, la/il Responsabile di Area/Settore, coadiuvata/o dalle proprie collaboratrici e dai propri collaboratori, valuta sia le richieste di mobilità esistenti presso la propria Area/Settore che quelle di altra provenienza raccolte tramite l'elenco del personale in mobilità. Se emergono disponibilità, il Responsabile, tramite i propri collaboratori, comunica il cambiamento di servizio o di ruolo all'Area Risorse Umane e ne dà comunicazione all'Unità Gestione Sistemi Informativi e all'Unità Gestione Privacy.

Qualora, invece, non emergano adeguate disponibilità interne alla Cooperativa, le/i Responsabili di Area/Settore, attraverso le/i referenti del personale, e le/i Responsabili delle Aree di Staff si rivolgono

all'Area Risorse Umane per attivare il percorso definito per la ricerca di nuovo personale.

4.2 RICERCA E SELEZIONE

Le Aree/Settori hanno un loro staff interno dedicato alla selezione, assunzione e gestione del personale (con l'individuazione di specifiche/ci addette/i all'espletamento del procedimento), mentre per le Aree di Staff sono le/gli stesse/i Responsabili a curare le fasi di acquisizione di nuovo personale.
Il processo di selezione si articola come segue.

a) Raccolta candidature

Le candidature che entrano a far parte del data base a disposizione del servizio di ricerca e selezione dell'Area Risorse Umane possono pervenire tramite diverse modalità:

- spontaneamente, attraverso l'apposita sezione del sito CADIAI;
- a seguito di campagne verso l'esterno promosse tramite diversi canali di comunicazione della Cooperativa;
- mediante campagne promosse utilizzando motori di ricerca specializzati (Linkedin, Indeed, e così via).

b) Richieste di personale

Le/gli addetti di ciascuna Area/Settore formalizzano le richieste di personale in un'apposita comunicazione in cui indicano al Servizio Ricerca e Selezione: tipo di profilo professionale, ambito operativo, data di richiesta della domanda, tempi di risposta, tipologia di contratto, ecc.

c) Selezione

Se nella banca dati al momento disponibile vi sono profili corrispondenti il Servizio Ricerca e Selezione procede alla loro valutazione, indicando quelli individuati all'Area/Settore che ha formalizzato la richiesta; in caso contrario si attivano le diverse iniziative di ricerca verso l'esterno sopra citate per acquisire la disponibilità di ulteriori profili nell'archivio.
L'analisi della banca dati interna avviene prendendo in esame le candidature nei tempi più brevi possibili e codificandole attribuendo loro uno "status" volto a identificare sia la fase del percorso conoscitivo che il livello di interesse per la candidatura. Lo status è utile per eliminare a livello preliminare i profili non pertinenti e per mettere in evidenza quelli invece tenuti in considerazione per approfondimenti successivi.
1° colloquio: il Servizio Ricerca e Selezione dell'Area Risorse Umane svolge in modo continuativo un'attività di valutazione delle risorse contattando per un primo colloquio le persone che, sulla base di titoli, capacità e competenze predefinite, e, nel caso vi siano specifiche esigenze riferite all'utenza dei servizi, genere, appaiono avere, secondo il curriculum presentato, caratteristiche congruenti con le richieste di personale in essere in quel momento. La scelta della tipologia di profilo a cui dare priorità si basa sia sul fabbisogno medio della Cooperativa che sulle specifiche richieste inoltrate per iscritto dalle Aree/Settori. Questo colloquio mira a presentare la Cooperativa nel suo complesso, con specifico riferimento agli ambiti di intervento per cui viene svolta la selezione, a verificare la congruenza dei requisiti della persona candidata con la posizione da ricoprire e la sua disponibilità ad operare nei servizi della Cooperativa, tramite l'approfondimento curricolare e l'analisi di altre compatibilità (anagrafiche, logistiche, ecc.). Il colloquio viene svolto seguendo la traccia della "Scheda colloquio selezione", sulla quale vengono apposte annotazioni rispetto alle informazioni più rilevanti raccolte utili alla determinazione del livello di adeguatezza riscontrabile nella persona candidata. Al termine del colloquio l'addetta/o alla selezione, valutate le caratteristiche complessive della persona candidata, ne aggiorna lo status inserendolo tra le "risorse" oppure tra i "non idonei".
Il 1° colloquio viene svolto normalmente dall'addetta/o alla ricerca e selezione, ma non in via esclusiva. Si possono infatti verificare situazioni (assenza prolungata dell'addetta/o alla selezione, situazioni di emergenza, ecc.) in cui il 1° colloquio può essere svolto direttamente da una/un addetta/o al Personale di Area/Settore.

2° colloquio: questa fase è attivata al momento della individuazione da parte del Servizio Ricerca e Selezione dell'Area Risorse Umane di un profilo coerente con i requisiti definiti dall'Area/Settore nella comunicazione di richiesta.
L'addetta/o al personale di Area/Settore esamina la candidatura proposta dal Servizio Selezione e Ricerca ritenuta più adeguata tra quelle alle quali è stato attribuito lo status di "risorsa".
L'incontro ha l'obiettivo di valutare se la persona candidata è in possesso di tutti i requisiti ritenuti necessari e di verificare se le sue competenze complessive siano adeguate all'assunzione dei compiti e delle mansioni previste per lo specifico ruolo da ricoprire. A sintesi di quanto emerso da questo 2° colloquio viene compilata la seconda sezione della "Scheda colloquio selezione" ed aggiornato lo status della persona candidata (può essere fatta una proposta di assunzione, può rimanere una risorsa, ecc.).
L'addetta/o al Personale di Area/Settore, quando le specificità di un Servizio lo rendono opportuno, può invitare la persona candidata ad un colloquio di ulteriore approfondimento con la/il Responsabile del Servizio e/o la/il Tecnico di riferimento per poter disporre di più elementi per la valutazione finale.
Per il personale operante nelle Aree di Staff le attività di selezione e assunzione vengono condotte dalle/i rispettive/i Responsabili attraverso le medesime procedure, analoghi strumenti ed interlocutrici/tori.
Quando dal 2° colloquio consegue la formulazione della proposta di assunzione, l'Area/Settore/Area di Staff verifica inoltre con la persona la compatibilità delle mansioni e degli orari della proposta contrattuale con le esigenze di conciliazione personali.
Durante i colloqui, seppur è possibile vengano raccolte informazioni sulle eventuali esigenze di conciliazione vita-lavoro, non vengono in nessun caso effettuate richieste relative a temi quali il matrimonio, la gravidanza o le responsabilità di cura che rappresentino un vincolo per la persona candidata.

d) Assunzione

Completata la fase di selezione con l'individuazione di un profilo viene effettuata la proposta di assunzione costruita sulla base dei seguenti criteri:

- attribuzione del livello e dell'inquadramento economico in stretta coerenza con quanto previsto dal CCNL di categoria (nazionale e territoriale);
- attribuzione di istituti o indennità definiti dalla Cooperativa ad integrazione di quanto previsto dal CCNL (indennità aggiuntiva per funzione, integrazioni economiche per specifiche figure professionali, e così via);
- valorizzazione di titoli ed esperienze acquisiti in specifici servizi o attività.

La coerenza dell'applicazione dei criteri con le normative e le prassi definite dalla Cooperativa viene assicurata attraverso un percorso strutturato che rappresenta un meccanismo di controllo: l'Area che propone l'inquadramento lo sottopone all'Area Risorse Umane che nell'elaborazione della pratica di assunzione necessariamente verifica la corrispondenza ai requisiti richiesti, allo scopo di evitare sia errori accidentali, sia trattamenti differenziati o discriminatori.
Qualora la proposta venga accettata, l'addetta/o al Personale di Area/Settore o il Responsabile dell'Area di Staff coinvolto nella ricerca avvia la fase di assunzione della persona candidata.
La definizione della proposta di assunzione e la sua accettazione aprono una fase più prettamente "amministrativa" connotata da un importante momento informativo nel quale alla persona candidata viene illustrata e consegnata la "cartellina per neo assunti", provvedendo ad espletare le attività previste per l'assunzione dall'Istruzione Operativa "Assunzione, gestione e dimissione del personale". L'Area/Settore consegna inoltre al Servizio Gestione Sistemi Informativi il modulo "Richiesta accessi informatici aziendali". Successivamente verifica gli eventuali corsi in materia di salute e sicurezza già sostenuti e il possesso dei corrispondenti attestati, li acquisisce e li invia al Servizio Prevenzione e Protezione affinché ne confermi la validità; nel caso in cui non vi sia evidenza dell'effettuazione di percorsi, vengono consegnate alla persona le credenziali per accedere alla Formazione Lavoratori parte generale in e-learning e pianificata la sua partecipazione alla Formazione Lavoratori sui rischi specifici. Concorda poi una data per la prima visita

medica per la valutazione dell'idoneità alla mansione.
Fornisce, infine, alla persona l'elenco dei documenti necessari per l'assunzione e fissa un appuntamento con il Servizio Amministrazione del Personale e Paghe dell'Area Risorse Umane per l'atto formale di assunzione.
Nel giorno stabilito l'addetta/o al personale dell'Area/Settore, o il Responsabile dell'Area di Staff, dopo aver controllato completezza e precisione dei dati della persona candidata e aver anticipato le condizioni generali del contratto da stipulare al Servizio Amministrazione del Personale e Paghe, vi accompagna la persona, munita della documentazione richiesta, per l'assunzione.
L'addetta/o all'assunzione del Servizio Amministrazione del Personale e Paghe provvede a verificare la presenza di tutti i documenti necessari e la corrispondenza tra quanto indicato sul modulo "Elementi necessari per l'assunzione" e quello che viene consegnato.

A completamento della documentazione il Servizio Amministrazione del Personale e Paghe fornisce ulteriori informazioni sulle retribuzioni mensili in vigore, sulla riforma previdenziale con contestuale consegna del modulo ministeriale per effettuare la scelta, sulle condizioni economiche in caso di malattia e sulle procedure necessarie da attivare in caso di infortunio o gravidanza.
Vengono inoltre richiesti alcuni dati essenziali rispetto ai carichi familiari e all'eventuale diritto a percepire o meno gli assegni familiari.
Tutti i documenti ricevuti per l'assunzione vengono inseriti nell'apposita cartella matricolare sulla quale vengono altresì annotati i dati principali della persona neo-assunta.
All'ingresso della persona neo assunta la/il Responsabile del servizio di destinazione ha il compito di presentare tutte le informazioni necessarie, comprese quelle in materia di salute e sicurezza, di consegnare gli eventuali Dispositivi di Protezione Individuale e di adempiere alle attività previste per questa fase dalla Istruzione Operativa "Assunzione, gestione e dimissioni del personale".

4.4 INSERIMENTO

Si tratta di un percorso strutturato finalizzato a guidare e monitorare il periodo di inserimento della persona neo assunta:

- per trasmettere tutte le informazioni necessarie allo svolgimento delle sue mansioni, comprese quelle in materia di salute e sicurezza e di privacy;
- per verificare con la lavoratrice o il lavoratore la completa acquisizione delle informazioni necessarie all'esercizio del ruolo assegnato;
- per valutare sotto il profilo operativo l'adeguatezza della persona neo assunta nello svolgimento dei compiti previsti all'interno del servizio.

A tal fine viene previsto (quando possibile) un periodo di affiancamento non operativo sul servizio ed un tutoraggio che, pur differenziandosi per tempi e modi a seconda dell'Area/Settore o Servizio di riferimento, caratterizza l'ingresso in ogni servizio della Cooperativa.
Per documentare e valutare il percorso di inserimento ci si avvale del modulo "Pianificazione dell'affiancamento/inserimento in servizio", strumento che serve per verificare la corretta esecuzione della fase di affiancamento. L'avvenuto addestramento all'utilizzo delle attrezzature e/o ausili viene documentato nel modulo "Registrazione addestramento". Attraverso il "Questionario di verifica sull'andamento del percorso di inserimento" la lavoratrice o il lavoratore è chiamata/o ad esprimere la sua valutazione rispetto alle informazioni ricevute nel periodo di affiancamento e ad esplicitare eventuali necessità di approfondimento.
La valutazione finale sull'idoneità della persona allo svolgimento dei compiti affidati è curata dalla/dal Responsabile del Servizio mediante compilazione di un'apposita scheda contemplata dal gestionale in uso che prevede la rilevazione delle caratteristiche emerse nelle diverse aree osservate. Entro lo scadere del periodo di prova, la/il Responsabile del Servizio, sulla base delle rilevazioni riportate nella scheda e di

eventuali ulteriori elementi, fa pervenire gli esiti dell'inserimento all'Area/Settore di pertinenza. La conferma o meno nel ruolo avviene, normalmente, in base al raggiungimento del punteggio minimo necessario, ma la/il Responsabile di Area/Settore, in presenza di elementi o situazioni particolari, può prescindere dal dato numerico e decidere in autonomia rendendo espliciti i motivi di tale scelta.
I documenti citati sono strutturati in modo da monitorare con efficacia le figure professionali ritenute prioritarie per la gestione dei servizi (Educatori, OSS, ecc.).
Nel caso di profili professionali che, per le loro specifiche caratteristiche, non rientrino nei parametri contemplati nel modulo "Pianificazione dell'affiancamento/inserimento in servizio" (ad es. figure amministrative, di coordinamento, sanitarie, ecc.), si utilizza il modulo "Pianificazione dell'affiancamento/inserimento in ruolo". Al termine del periodo di affiancamento/inserimento viene richiesta la compilazione del "Questionario di verifica sull'andamento del percorso di inserimento (per uffici sede e coordinamento servizi)". Anche in relazione a questi profili viene effettuata una valutazione con le stesse modalità sopra illustrate.

Il percorso di inserimento non è pianificato e tenuto sotto controllo solo nel caso della persona neo assunta, ma anche in relazione ad altre casistiche che coinvolgono il personale già in forza, in particolare:

- personale in mobilità spostato ad altro servizio o ufficio;
- variazione di ruolo o percorso di carriera;
- rientro da maternità o paternità;
- rientro da assenza prolungata.

Contenuti e durata dell'inserimento, e conseguenti strumenti di tenuta sotto controllo dello stesso, variano dipendentemente dalle informazioni e dalle nuove competenze da acquisire.

4.5 REGISTRAZIONE PRESENZE

Le lavoratrici e i lavoratori, dal giorno dell'assunzione, sono tenute/i alla compilazione del foglio per la rilevazione delle ore di lavoro svolte quotidianamente (modulo "Foglio Presenze" o rilevazione elettronica tramite gestionale). Il "Foglio Presenze" deve essere compilato ogni giorno riportando il numero di ore lavorate, le giornate di ferie, malattia e altre specificità inerenti all'attività lavorativa espressamente previste dal modulo. Entro il giorno 5 del mese successivo, le/i Responsabili di Servizio inviano i fogli presenze, corredati già dai dati riepilogativi, al Servizio Amministrazione del Personale e Paghe che completa i dati necessari inserendo le voci di propria competenza.
I dati vengono inseriti o attraverso un programma informatico che registra le timbrature dei cartellini marcatempo o direttamente dalle/i Responsabili dei Servizi che manualmente riportano i contenuti dei fogli presenze. Una volta effettuate tutte le verifiche per accertare la correttezza di tutte le imputazioni, si chiude la fase di raccolta dati e si procede alla loro elaborazione per ottenere le buste paga. Vengono inoltre prodotti report ed informazioni varie utili per la programmazione dell'attività complessiva e la gestione dei servizi.

4.6 DIMISSIONE

Quando una lavoratrice o un lavoratore decide di dimettersi, è tenuto a darne preavviso alla/al Responsabile di Servizio di riferimento che, previo colloquio con la persona dimissionaria, informa la/il Responsabile di Area o il suo staff. Qualora, tuttavia, le dimissioni giungano direttamente al Servizio Amministrazione del Personale e Paghe, quest'ultimo informa l'Area/Settore di pertinenza.
Quest'ultima, in entrambi i casi, verifica tempi, data e modalità di dimissione, e conseguentemente valuta se il periodo di preavviso individuato comporti oneri per una delle parti.
La persona dimissionaria, così come previsto dalla normativa vigente, non può dare alcuna dimissione senza l'obbligatorio percorso delle dimissioni on line, semmai avvalendosi di intermediari abilitati (es. dai patronati).
Una volta ricevuto a mezzo PEC il documento di dimissione online, l'Area Risorse Umane, previa verifica di alcuni dati con l'Area/Settore di pertinenza, provvede a tutti gli atti necessari e alla restituzione dei

documenti richiesti e comunica la dimissione all'Unità Gestione Sistemi Informativi al fine di disattivare gli eventuali accessi (a email, a cartelle aziendali su server, a gestionali, etc.). Analogamente, per il personale operante nelle Aree di Staff il riferimento è costituito dalle/dai rispettive/i Responsabili.
In questa fase e oltre, la lavoratrice o il lavoratore può richiedere copia della propria cartella sanitaria e scaricare dal gestionale eventuali attestati relativi ai corsi di formazione frequentati in materia di salute e sicurezza.
L'eventuale dimissione di una socia lavoratrice o di un socio lavoratore è altresì disciplinata dalle leggi dello Stato e dallo Statuto della Cooperativa che stabiliscono i tempi per la cessazione dello status di socia/o e per la restituzione della quota sociale (vedi modulo "Dimissioni da socia/o"). Tutti i passaggi previsti per le dimissioni sono dettagliate nell'Istruzione Operativa "Assunzione, gestione e dimissione del personale".

4.7 ELABORAZIONE DI DATI E STATISTICHE SUL PERSONALE

Dai dati relativi alla gestione del personale[1], l'Area Risorse Umane estrapola le informazioni necessarie per la elaborazione di report e statistiche da presentare alle Aree produttive, al Consiglio di Amministrazione, alla Direzione, al Servizio Prevenzione e Protezione, al Comitato per la Responsabilità Sociale, al Comitato per la Salute e la Sicurezza, all'Organismo di Vigilanza, al Comitato Pari Opportunità e ad altri eventuali funzioni o organi interessati, quali elementi per il controllo ed il riesame delle attività della Cooperativa.
Questa operazione è indispensabile per consentire all'Area Amministrazione Generale di:
- elaborare il controllo di gestione complessivo della Cooperativa;
- elaborare le linee per il budget preventivo.

A loro volta le Aree/Settori si avvalgono dei dati prodotti al fine di:
- elaborare il budget preventivo;
- effettuare un accurato controllo di gestione;
- quantificare il tasso di assenteismo e di turn over presente nei servizi e definire il fabbisogno di personale negli stessi.

Per consentire un monitoraggio e una valutazione dello stato delle pari opportunità nella Cooperativa, i dati riferiti al personale, ove pertinenti, vengono disaggregati (es. per genere, nazionalità, ecc.).
Inoltre, in coerenza con il Modello Organizzativo predisposto in ottemperanza al D. Lgs. 231/2001, l'Area Risorse Umane provvede alla comunicazione all'Organismo di Vigilanza (ogni sei mesi o a richiesta) delle statistiche inerenti: assunti e dimessi, applicazione di sistemi premianti/incentivanti a lavoratori. In materia di salute e sicurezza sul lavoro vengono messi a disposizione del Servizio Prevenzione e Protezione gli elenchi degli infortuni registrati e delle sanzioni disciplinari eventualmente comminate al personale per inosservanza delle norme sulla sicurezza ex D. Lgs. 81/2008. In caso di infortuni gravi (e comunque sempre in caso di prognosi pari o superiore a 60 giorni) l'Area Risorse Umane dà immediata comunicazione al Servizio Prevenzione e Protezione e all'Organismo di Vigilanza.
Infine, al Comitato per la Responsabilità Sociale vengono periodicamente (ogni sei mesi o, anche, a richiesta) comunicati dati riguardanti: l'età e la nazionalità del personale, la mobilità, le richieste di aspettativa, gli infortuni, le ore di sciopero e quelle dedicate all'attività sindacale, i procedimenti disciplinari, le ore di straordinario e di ferie residue, il numero di mancati riposi, la retribuzione.

4.8 GESTIONE DEL PERSONALE: RILEVAZIONE DEI FABBISOGNI, VALUTAZIONE E PERCORSI DI CARRIERA

La gestione del personale è posta in capo alla/al Responsabile di Area/Settore di appartenenza che si avvale della collaborazione dell'Area Risorse Umane.
L'Area Risorse Umane costituisce punto di riferimento per la predisposizione del contratto, i rapporti con gli enti previdenziali e l'elaborazione della busta paga; ha anche il compito di predisporre strumenti per la

[1] Dati relativi alle tipologie di contratti, alle qualifiche, all'assenteismo per malattia e infortunio, al residuo ferie, al costo del personale, allo stato delle assunzioni, alla situazione per genere, alla situazione maschile per ognuna delle professioni, alla formazione, alla promozione professionale, ai livelli, ai passaggi di categoria o di qualifica, ad altri fenomeni di mobilità, all'intervento della CIG, ai licenziamenti, ai prepensionamenti e pensionamenti, alla retribuzione effettivamente corrisposta.

valutazione ed il bilancio delle competenze professionali e realizzare interventi formativi e di qualificazione professionale rivolti a tutto il personale.
Ciascuna Area/Settore rileva periodicamente i fabbisogni di lavoratrici e lavoratori, sia rispetto alle esigenze relative all'erogazione del servizio che ai bisogni personali, tramite:

- incontri periodici dell'equipe di lavoro, incontri di Coordinamento Tecnico ed Amministrativo;
- somministrazione dei questionari per l'autovalutazione delle competenze e la rilevazione del fabbisogno formativo;
- somministrazione del "Questionario di soddisfazione del personale";
- controllo del tasso di assenteismo interno ai servizi e di turn-over interno alla Cooperativa;
- somministrazione del "Questionario sulla salute e sicurezza sul lavoro".

Gli ultimi tre interventi sono finalizzati a rilevare il clima interno e il benessere di cui gode l'organizzazione nel suo complesso e a individuare eventuali azioni di miglioramento.

Gli esiti di tali rilevazioni, tra le altre cose, vengono utilizzati per lo sviluppo di politiche volte a valorizzare il personale ed incrementare le conoscenze e competenze professionali delle lavoratrici e dei lavoratori attraverso:

- la promozione di condizioni di lavoro che, compatibilmente con le esigenze del servizio, consentano la miglior conciliazione vita-lavoro con particolare attenzione ad assicurare pari opportunità. In particolare, ad esempio, pur essendo gli orari delle riunioni di lavoro definiti in base all'organizzazione del servizio, viene garantita la compatibilità con la conciliazione dei tempi di vita familiare e personale prevedendo anche la possibilità della partecipazione on line. Nei servizi in cui, in forza della natura stessa del servizio (SAD, Centri Diurni, Servizi Educativi Territoriali, Nidi d'Infanzia, e così via), le lavoratrici e i lavoratori sono in gran parte part time, poi, le riunioni di lavoro sono organizzate fuori dall'orario di prestazione diretta in modo da essere accessibili a tutte e a tutti all'interno del loro orario di lavoro o ad un'eccedenza dello stesso. Nelle strutture a turni (Residenze) vengono organizzate, invece, in orari che consentono la massima partecipazione (orario del riposo delle persone utenti, …) oppure replicate. Sono, inoltre, contemplate, se compatibili con la tipologia di servizio:
    - ulteriori misure per garantire l'equilibrio vita-lavoro (come, ad esempio, l'esonero temporaneo da alcuni turni) rivolte a tutte/i le/i dipendenti;
    - la concessione del part-time a chi ne faccia richiesta;
    - l'offerta della flessibilità di orario (come, per esempio, nel caso dei cambi turno);
    - la revisione periodica delle esigenze di flessibilità del personale;
    - la possibilità, per il personale degli uffici, di smart working/telelavoro o di altre forme di lavoro flessibile, e orario elastico;
- l'organizzazione di attività di formazione volte a potenziare attitudini e competenze di lavoratrici e lavoratori e la realizzazione di percorsi di qualificazione professionale;
- l'aggiornamento costante dei curricula professionali del personale;
- la pianificazione di percorsi di carriera, assicurando la non discriminazione e le pari opportunità nello sviluppo professionale e nelle promozioni, basando queste ultime esclusivamente sulle capacità ed i livelli professionali.

Le/i Responsabili di Area/Settore e delle Aree di Staff si avvalgono dei percorsi e degli strumenti sopra descritti anche per raccogliere tutti i dati relativi al personale utili ad una valutazione delle specifiche caratteristiche e delle potenzialità riscontrate.
Sulla base degli elementi e delle informazioni emerse vengono predisposti percorsi di carriera che si possono sviluppare sia in senso orizzontale che in senso verticale. Nel primo caso significa valorizzare al massimo il profilo individuale di ciascuna persona, sia nell'ambito delle richieste di mobilità che in quello della disponibilità di nuove opportunità di lavoro, mediante una collocazione il più possibile coerente con le sue competenze e le sue potenzialità. Per quanto riguarda invece i percorsi di carriera in senso verticale

ciascuna Area/Settore, una volta individuata la figura con i requisiti per l'attribuzione di nuovi incarichi o ruoli interni di più ampia responsabilità, la propone alla Direzione che, valutato il rispetto delle pari opportunità nella procedura, esprime in merito le proprie valutazioni.
Spetta comunque alla/al Responsabile di Area/Settore la valutazione finale in merito.
Mensilmente le Aree produttive e di Staff (o l'Area Risorse Umane) comunicano le variazioni dello status della lavoratrice o del lavoratore (inquadramento, centro di costo, mansioni, aspettative, maternità) anche quando comportino esclusivamente modifiche agli accessi sui server/gestionali di Cadiai all'Unità Gestione Sistemi Informativi utilizzando il modulo "Richiesta accessi informatici aziendali".
Qualora le nuove funzioni attribuite comportino variazioni di inquadramento o introduzioni di indennità economiche, l'Area Risorse Umane nell'elaborazione della pratica amministrativa effettua un controllo sulla corretta applicazione dei criteri fissati ai fini di un equo trattamento di tutto il personale.
Le informazioni e i percorsi intrapresi inerenti alle carriere individuali vengono successivamente comunicati al Consiglio di Amministrazione, con esclusione dei ruoli direttivi per i quali è prevista la nomina da parte del Consiglio stesso.
Per quanto riguarda i ruoli direttivi oltre a quanto riportato nel documento "Profili professionali e funzionali in CADIAI" si tiene conto del valore della differenza nei processi decisionali di vertice e quindi si tende ad assicurare un equilibrio di genere.

4.9 PERSONALE DI CITTADINANZA EXTRA UNIONE EUROPEA

Nella continuità del rapporto di lavoro, la Cooperativa monitora e sollecita il rinnovo della Carta di Soggiorno che si avvicini a scadenza: almeno 60 giorni prima della data di scadenza, l'Area Risorse Umane invia un telegramma alla/al dipendente, segnalando che presso la Cooperativa è già disponibile, e sarà consegnata in busta paga, la documentazione per la richiesta del rinnovo della Carta. Altresì nel telegramma si fa presente la necessità per CADIAI di ricevere la Ricevuta della Raccomandata con la quale la lavoratrice o il lavoratore fa richiesta di rinnovo. Con la ricevuta si procede al controllo sul sito della Questura dello stato del permesso. Quando lo stato risulta "rinnovato", si comunica alla lavoratrice o al lavoratore di procedere con il ritiro in Questura e di consegnarne copia all'Area Risorse Umane.

5. ARCHIVIAZIONE

I documenti citati in questa procedura sono conservati come indicato all'interno della procedura gestionale "Gestione dei Documenti".