POLICY AZIENDALE

La Cooperativa DIDASCO opera dal 1994 nel settore della diagnosi e della riabilitazione dei disturbi cognitivi, disturbi neuropsicologici e disarmonie dello sviluppo. Inoltre fornisce servizi socioassistenziali a persone con disabilità.

Per il perseguimento del proprio scopo, pertanto, svolge tutte le attività a ciò necessarie tra le quali – per quanto qui interessa:

- le procedure legate all'acquisizione e alla gestione delle risorse umane
- l'approvvigionamento degli strumenti, dei materiali, dei servizi e dei lavori
- la formazione del personale
- l'organizzazione ed erogazione dei servizi

Nello svolgimento delle proprie attività, l'Azienda gestisce differenti tipologie di dati personali come quelli di seguito elencati a titolo esemplificativo:

1. ***dati anagrafici in senso stretto*** riferibili ai lavoratori ed ai loro familiari, ai legali rappresentanti di imprese fornitrici di beni e servizi nonché di professionisti e consulenti esterni, ecc.;
2. ***dati legali e giudiziari*** riferibili alle persone fisiche operanti all'interno dell'azienda, di imprese fornitrici di beni, servizi e lavori quali i legali rappresentanti, i singoli soci, i singoli componenti degli organi amministrativi e di controllo ed i rispettivi familiari conviventi;
3. ***dati relativi alla salute*** dei lavoratori inquadrati ad ogni livello aziendale;
4. ***dati atti a rivelare l'appartenenza sindacale dei lavoratori***;
5. ***dati bancari*** dei lavoratori, dei fornitori e dei clienti;
6. ***dati biometrici***, quali ad esempio le fotografie dei lavoratori dipendenti o dei professionisti o dei consulenti esterni, necessarie eventualmente all'elaborazione dei tesserini di riconoscimento per l'accesso in sede ovvero nelle sedi dislocate sul territorio nazionale e comunitario. Non si è rilevato, invece, l'uso di impronte digitali o della topografia della mano.

Al trattamento effettivo di tali dati si aggiunge il trattamento potenziale (in quanto sino ad ora mai verificatosi) di ***dati atti a rivelare le convinzioni religiose dei lavoratori***, per il trattamento dei quali, a fini prudenziali, si richiede in via anticipata il consenso esplicito dell'interessato.

Inoltre, relativamente alle specifiche finalità perseguite dall'Azienda gli ulteriori dati personali oggetto di trattamento da parte della predetta azienda sono elencati a titolo esemplificativo nella tabella che segue:

Tipologia	*Descrizione del trattamento dei dati*
Dati generali	Tutte le informazioni generali che possono essere desunte da documenti indirizzati all'ente in entrata e/o in uscita e delibere o verbali del Consiglio di Amministrazione
Dati patrimoniali	L'inventario dei beni, la loro classificazione e le varie informazioni riconducibili alla situazione patrimoniale dell'ente
Dati tecnici	Informazioni sulle infrastrutture, sulla organizzazione e controllo delle attività di manutenzione degli impianti e degli stabili
Dati contabili	Tutte le informazioni riguardanti la gestione contabile (compresi archivi clienti e fornitori), fatturazione attiva e passiva, contabilità ordinaria e fiscale
Dati amministrativi del personale	Fascicolo del personale dipendente con relativa documentazione di assunzione e tutte le informazioni amministrative raccolte per il reclutamento e la selezione, la predisposizione del contratto di lavoro, lo svolgimento della professione e la gestione del rapporto di lavoro.
Dati retributivi del personale	Banca dati retributiva per l'elaborazione delle paghe e stipendi, il trattamento di dati previdenziale e fiscali

In armonia con l'ottica di responsabilizzazione e di rischio del GDPR, di primaria importanza - logica prima ancora che giuridica - è la giusta percezione del ***"peso" del dato personale***, ossia della circostanza che non tutti i dati personali siano uguali e che, pertanto, non tutti debbano essere protetti allo stesso modo: a titolo esemplificativo, un dato relativo alla salute è più delicato di altri e, conseguentemente, l'Azienda ha ideato ed applicato un sistema di protezione più solido.

Sotto tale profilo, un ruolo cruciale rivestono la **cifratura dei dati** e la **pseudonimizzazione**, due misure di sicurezza che si rivelano preziose soprattutto in caso di attacco agli archivi o in occasione di *data breach*, smarrimento o furto dei dispositivi e altre fuoriuscite non volute di informazioni, che si pone in pratica sia quando il trattamento avviene con strumenti cartacei che con strumenti informatici.

La base giuridica del trattamento di tali dati è rappresentata da:

- l'adempimento degli obblighi contrattuali e pre-contrattuali di cui l'Azienda è parte;
- l'adempimento degli obblighi di Legge cui la stessa è tenuta;
- per finalità amministrativo-contabili;
- legittimo interesse del Titolare.

Il consenso prestato dall'Interessato preliminarmente al trattamento stesso, il quale è revocabile liberamente ed in qualsiasi momento

Ogni funzione aziendale tratta i dati personali sopra elencati limitatamente alla propria competenza, come definita dall'organigramma aziendale.

Quando gestiti in ***forma cartacea***, tutti i documenti sono custoditi in armadi e/o schedari chiusi a chiave all'interno delle stanze dei relativi Responsabili e/o Incaricati, anch'esse chiuse a chiave.

Sono impartite a tutti gli incaricati precise istruzioni sul trattamento dei dati e delle pratiche cartacee, in particolare la *duplicazione elettronica* mediante scansione dei documenti cartacei, onde prevenirne la distruzione totale accidentale e la *pseudonimizzazione* mediante l'archiviazione dei documenti basata sul numero di matricola e/o codici univoci che non consentono l'immediata identificazione della persona dell'interessato, la quale è consentita solo a determinati soggetti, a tal fine autorizzati, cui sono accessibili le tabelle di conversione nome/matricola.

Regolarmente i Responsabili di ciascuna funzione controllano che le regole di tenuta della documentazione cartacea siano osservate da tutti gli incaricati sottoposti.

Quando gestiti in ***forma elettronica***, i dati ed i relativi documenti vengono trattati mediante *personal computers*, fissi e portatili, nonché *smartphones* messi a disposizione del personale ed utilizzati in esclusiva da ciascun incaricato. I dispositivi informatici sono tutti protetti da un doppio ordine di *passwords*: la prima richiesta all'atto dell'accensione del terminale e la seconda per l'accesso alle piattaforme informatiche gestionali.

Entrambe le *passwords* sono conoscibili esclusivamente dall'affidatario del dispositivo informatico e dall'Amministratore del sistema.

Nel caso di utilizzo di un PC diverso dal proprio, ogni incaricato deve, comunque, ricollegarsi alla rete con le proprie credenziali.

Tutte le credenziali di accesso sono custodite da ciascun affidatario con la massima attenzione e, in caso di loro furto o smarrimento, è previsto il coinvolgimento immediato del Responsabile della Protezione dei Dati (DPO) ove nominato ai sensi dell'art. 37 del Regolamento UE 679/2016 e del legale rappresentante dell'Ente che, senza indugio, richiedono l'immediato intervento dell'Amministratore di sistema affinché blocchi le credenziali oggetto di furto e/o smarrimento, verifichi l'assenza *medio tempore* di eventuali accessi non autorizzati e fornisca nuove credenziali di autenticazione che, al primo accesso da parte dell'incaricato, dovranno essere modificate a sua cura e sotto la sua esclusiva responsabilità.

L'Azienda, inoltre, si avvale ~~di *social networks* per scopi divulgativi e informativi e~~ di un proprio sito internet ufficiale, nell'ambito del quale i dati comunicati dall'utenza o comunque raccolti nel corso della navigazione non sono di norma accompagnati da alcuna informazione personale aggiuntiva rispetto agli usuali dati la cui trasmissione è implicita nell'uso dei protocolli di comunicazione di Internet (quali ad esempio nomi di dominio, indirizzi IP, sistema operativo utilizzato, tipo di *device* e di *browser* utilizzati

per la connessione) e vengono trattati per gestire esigenze di controllo delle modalità di utilizzo dello stesso, accertare responsabilità in caso di ipotetici reati informatici e ricavare informazioni statistiche anonime sull'uso del sito. La base giuridica che legittima il trattamento di tali dati è la necessità di rendere utilizzabili le funzionalità del sito a seguito dell'accesso dell'utente.

Nel caso di invio da parte dell'utenza del sito informatico di *curriculum vitae* a scopi di *recruiting* i dati personali aggiuntivi sono raccolti e trattati esclusivamente per finalità di selezione ed in tal caso la base giuridica che legittima il trattamento è l'esecuzione di misure precontrattuali adottate su richiesta dello stesso candidato.

Qualora sia necessario o strumentale per l'esecuzione delle specifiche finalità, i dati personali, oltre che dal personale aziendale preposto, sono comunicati a destinatari nominati ai sensi dell'art. 28 del GDPR, che li trattano in qualità di Responsabili e/o in qualità di persone fisiche che agiscono sotto l'autorità del Titolare e del Responsabile al fine di ottemperare ad obblighi di legge, a contratti o alle finalità connesse. Precisamente, i dati possono essere comunicati ai seguenti destinatari: Pubbliche Amministrazioni, Enti Locali, Enti o Casse anche private di Previdenza e Assistenza (INPS, INAIL, INPDAP), Fornitori di Servizi, Istituti di Credito, Liberi Professionisti, Enti di Formazione, ecc..

L'elenco dei Responsabili del trattamento designati è costantemente aggiornato e disponibile presso la sede legale dell'Azienda e sui suoi portali informatici. In nessun caso i dati raccolti sono oggetto di diffusione e/o di trasferimento all'estero, né all'interno né all'esterno dell'Unione Europea.

Nel rispetto di quanto previsto dall'art. 5, comma 1, lett. e) del GDPR, i dati personali vengono conservati in una forma che consenta l'identificazione dell'interessato per un arco di tempo non superiore al conseguimento delle finalità per le quali i dati stessi sono trattati o in base alle scadenze previste dalle norme di legge.

La verifica sulla obsolescenza dei dati conservati in relazione alle finalità per cui sono stati raccolti viene effettuata periodicamente, sotto la vigilanza del Responsabile della Protezione dei dati (DPO) ove nominato o del personale all'uopo preposto.

Infine, alla luce della complessità e dell'incertezza del quadro normativo in vigore, l'Azienda ha inteso adottare un approccio prudenziale, rispettoso del GDPR oltre quanto strettamente dovuto attraverso:

- la richiesta del consenso esplicito dell'interessato, anche quando non strettamente necessario;
- l'espletamento della valutazione di impatto, ritenuta opportuna sebbene non obbligatoria;
- la nomina di Responsabili del trattamento "interni", al fine di garantire l'applicazione e la vigilanza capillari circa il rispetto del Regolamento.