



Brochure informativa
per i Soci e per i dipendenti
di Duemilauno Agenzia Sociale

REGOLAMENTO EUROPEO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

Gennaio 2019



DUEMILAUNO
AGENZIA SOCIALE

A COSA SERVE QUESTA BROCHURE INFORMATIVA

La finalità di questa sintetica brochure è di fornire a tutti i soci lavoratori e dipendenti di Duemilauno Agenzia Sociale - Soc. Coop. Soc. Impresa Sociale ONLUS (di seguito DMLAS) una prima informazione su quanto stabilito in materia di tutela e protezione dei dati personali dal **Regolamento (UE) 2016/679 (di seguito GDPR)** in vigore dal 28 maggio 2018.



CHE COSA È IL GDPR E FINALITÀ

GDPR indica **General Data Protection Regulation** ed è una normativa a livello europeo che si pone l'obiettivo di uniformare e normalizzare le diverse disposizioni che regolano il trattamento dei dati personali, disciplinando le modalità con cui i dati e le informazioni devono essere archiviate, protette e rese accessibili da parte delle aziende.

COME FUNZIONAVA PRIMA

Il riferimento era il D.Lgs 196/2003, "Codice per la protezione dei dati personali", con il D.Lgs 101/2018 è stato adeguato alle disposizioni del GDPR.

QUAL È L'AMBITO DI APPLICAZIONE DEL GDPR?

Il Regolamento si applica al trattamento dei dati personali di persone fisiche residenti nell'Unione Europea nell'ambito delle attività di un'azienda, di un'organizzazione o di un libero professionista. Si applica anche ad aziende extra Unione Europea che forniscono beni o servizi a residenti nell'Unione.



COSA SIGNIFICA TRATTAMENTO DEI DATI PERSONALI?

Per trattamento dei dati personali si intende 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, la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, la diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

Il concetto di trattamento coinvolge tutte quelle operazioni che implicano una conoscenza di dati personali.

QUALI SONO I DATI PERSONALI?

Per **Dati personali** si considerano tutte le informazioni relative ad un individuo e connesse sia alla sua vita privata che professionale o pubblica. Ad esempio il nominativo, la fotografia, l'indirizzo, le mail, i dati bancari, l'indirizzo IP dei computer, gli interventi sui siti web, sui social network, ecc.. **Il GDPR considera quindi dati personali tutti quelli che possono servire per identificare o rendere identificabile un individuo.**

Alcuni dati aziendali potrebbero essere dati personali, ad esempio: **mrossi@2001agsoc.it** è un dato personale in quanto può essere ricollegato a una persona fisica. Indirizzi mail come **info@2001agsoc.it** non sono invece considerati dati personali.





CI SONO DELLE CATEGORIE SPECIALI DI DATI PERSONALI?

Esistono i dati sensibili e i dati giudiziari. Di seguito una breve definizione:

> **Dati sensibili:** è una categoria speciale dei **dati personali** che rivelano l'origine razziale od etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'appartenenza sindacale, nonché quelli relativi alla salute o alla vita sessuale o l'orientamento sessuale. Il GDPR ha incluso in questo gruppo anche i **dati genetici** (ottenuti tramite analisi del DNA e RNA da un campione biologico della persona fisica in questione), **i dati biometrici** (es. impronta digitale, scansioni della retina e del viso, ecc..).

L'elaborazione dei dati sensibili è soggetta a trattamento speciale.

> **Dati giudiziari:** è un'ulteriore categoria di **dati personali** che rivelano l'esistenza, in capo all'interessato, di provvedimenti penali suscettibili di iscrizione nel casellario giudiziale, o la qualità di indagato o imputato.

In questo caso il trattamento può avvenire soltanto se autorizzati da espressa disposizione di legge o da provvedimento del Garante che descrivano compiutamente le finalità di rilevante interesse pubblico del trattamento, i tipi di dati trattati e le operazioni eseguibili. Tale trattamento può essere autorizzato solo qualora risulti indispensabile per "adempiere o esigere l'adempimento di specifici obblighi o eseguire specifici compiti previsti dalle leggi, dalla normativa dell'Unione europea, da Regolamenti o da Contratti collettivi, anche aziendali, e ai soli fini della gestione del rapporto di lavoro".



COSA COMPORTA L'APPLICAZIONE DEL GDPR PER LE AZIENDE?

Le Aziende che trattano dati personali devono:

- > **adottare** un *linguaggio semplice nella richiesta di consenso, nella raccolta dei dati personali e devono altresì essere chiare le finalità per le quali questi dati vengono richiesti;*
- > **salvaguardare i dati dalla distruzione, dalla perdita o dalla loro modifica** oltre a proteggerli da accessi non autorizzati attraverso l'adozione di comportamenti proattivi;
- > **documentare la valutazione del rischio e delle misure messe in atto per proteggere i dati personali;**
- > **notificare** (entro 72 ore) **ogni caso di perdita o furto o distruzione di dati.**



QUALI SONO I DIRITTI DEI CITTADINI RESIDENTI NELLA UE PREVISTI NEL GDPR?

- 1) **Sapere** se è in corso un trattamento di dati personali che li riguardano e di **essere informati sul perché i loro dati vengono raccolti e come vengono utilizzati** ed ottenere una copia di tali dati.
- 2) **Chiedere**, nei casi previsti dal Regolamento, **che i dati personali che li riguardano siano rettificati o cancellati, o che ne venga limitato il trattamento.**
- 3) **Chiedere che i dati personali che li riguardano possano essere trasferiti da un cliente/fornitore ad un altro.**
- 4) **Opporsi al trattamento dei dati personali per motivi** connessi alla propria situazione particolare, da specificare nella richiesta, oppure senza necessità di motivare l'opposizione, quando i dati sono trattati per finalità di marketing diretto.

LE FIGURE COINVOLTE



Chi è l' "INTERESSATO"

La persona fisica alla quale si riferiscono i dati personali e rispetto alla quale la normativa attribuisce specifici diritti.

Chi è il "TITOLARE DEL TRATTAMENTO" (Data Controller)

È "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". In sostanza il Titolare è colui che tratta i dati senza ricevere istruzioni da altri, colui che decide "perché" e "come" devono essere trattati i dati.

Il Titolare del trattamento non è, quindi, chi gestisce i dati, ma chi decide il motivo e le modalità del trattamento.

Chi è il "RESPONSABILE DEL TRATTAMENTO" (Data Processor)

È "la persona fisica, giuridica, pubblica amministrazione o ente che elabora i dati personali per conto del Titolare del trattamento". Si tratta di un soggetto, **distinto dal Titolare, che deve essere in grado di fornire garanzie al fine di assicurare il pieno rispetto delle disposizioni in materia di trattamento dei dati personali, nonché di garantire la tutela dei diritti dell'interessato.**

Chi è l' "INCARICATO DEL TRATTAMENTO"

Il GDPR non prevede espressamente la figura dell'incaricato, ma non ne esclude la nomina, facendo riferimento a persone autorizzate al trattamento dei dati sotto l'autorità diretta del Titolare o del Responsabile.

L'Incaricato, o l'Autorizzato, è **la persona fisica alla quale sono state fornite delle istruzioni operative per effettuare materialmente le operazioni di trattamento sui dati personali.**

Chi è il "RESPONSABILE PROTEZIONE DATI" - RPD (Data Protection Officer- DPO)

Il "Responsabile della protezione dei dati" è una figura con l'incarico di **assicurare una gestione corretta dei dati personali nelle imprese e negli enti, individuato in funzione delle qualità professionali e della conoscenza specialistica della normativa e della prassi in materia di protezione dati.**

È una figura rilevante, ma certamente non è il "centro" del sistema posto in essere dal GDPR, che nel nuovo ordinamento è sempre il Titolare del trattamento.





FAQ (Frequently Asked Questions) sul GDPR in DmlAS

1. Più nel dettaglio che finalità ha il GDPR?

La finalità ultima del GDPR è *la tutela del diritto alla protezione dei dati personali*, inteso come diritto fondamentale delle persone fisiche. *Si applica al trattamento dei dati personali. Non si applica ai dati aziendali, come il nome e l'indirizzo della società.* Tuttavia qualsiasi dato che si riferisce alle persone fisiche che lavorano in un'azienda è considerato **"personale"**, indipendentemente dal fatto che venga trattato in un contesto che si riferisce ad uno scambio commerciale di prodotti o servizi tra aziende.

2. Perché per DmlAS è importante il GDPR?

DmlAS nell'ambito delle sue attività risulta Titolare del Trattamento di dati personali e dati sensibili.

3. Quali sono gli ambiti di applicazione del trattamento di dati personali DmlAS?

Il trattamento dei dati personali in DmlAS si applica nello svolgersi delle attività interne di tipo amministrativo e delle attività operative.

4. Quali sono i dati personali che DmlAS tratta nelle attività di tipo amministrativo?

La maggior parte del trattamento dei dati nelle attività amministrative riguarda l'Ufficio Personale - Paghe: infatti in questi contesti vengono raccolte le pratiche di assunzione, l'elaborazione delle paghe, si gestiscono i rapporti di cessazione, ecc.. Risulta rilevante il trattamento di dati, anche sensibili, da parte dell'Ufficio Gestione Sicurezza dove viene effettuata l'elaborazione e conservazione della documentazione L. 81/08, (*documenti, cartelle mediche, ecc.*). Anche gli altri uffici facente parte dell'Area amministrativa (*Segreteria, Contabilità,*





Ufficio Rendicontazione, ecc.) nei loro compiti sono tenuti alla massima riservatezza nel trattamento dei dati personali in loro possesso. In questo ambito ci si avvale di consulenze (*Studi legali, Consulenti contabili/amministrativi, assistenza informatica, consulenza per il trattamento giuridico ed economico del personale, ecc.*). Per questi servizi sono state effettuate le nomine a Responsabile del Trattamento con l'indicazione dei dati da trattare.

5. Ci sono delle procedure particolari che DmlAS ha adottato per il trattamento dei dati nelle attività di tipo amministrativo?

Per ogni ufficio sono state predisposte le procedure e le istruzioni operative con l'indicazione dei dati da trattare e le modalità previste.

6. Quali sono i dati personali che DmlAS tratta nelle attività operative?

Sono tutti i dati relativi all'utenza: si tratta di dati personali (*nome e cognome, età, indirizzo, parenti, relazioni scolastiche quali PDP, pagelle, ecc.*) ed in diversi casi anche di dati sensibili (*documentazione attestante informazioni medico-sanitaria, ecc.*). Ovviamente, vista la vastità di tipologie d'utenza, i dati da trattare sono diversi da Servizio a Servizio e proprio per questo sono state predisposte delle applicazioni diverse nel trattamento dei dati.



7. Ci sono delle procedure particolari che DmlAS ha adottato per il trattamento dei dati nelle attività operative?

Per ogni Servizio vengono nominati dei Responsabili di Trattamento con l'indicazione dei dati da trattare e le modalità previste. Inoltre sono state predisposte delle istruzioni operative con l'indicazione per tutti gli Operatori di procedure specifiche da adottare nel Servizio nel quale lavorano, in particolare per la tutela dei dati in possesso.



8. Quale ruolo ha DmlAS per il trattamento dei dati nelle varie attività?

DMLAS nell'ambito amministrativo tratta i dati come Titolare del Trattamento in quanto decide **"perché"** e **"come"** devono essere trattati i dati. Nelle attività operative il trattamento è più articolato: **a)** nei Servizi privati DMLAS è Titolare del Trattamento; **b)** nei Servizi in appalto il Titolare è invece l'Ente appaltante. In quest'ultimo caso infatti DMLAS è Responsabile del Trattamento, deve essere pertanto in grado di fornire garanzie al fine di assicurare il pieno rispetto delle disposizioni in materia di trattamento dei dati personali, nonché di garantire la tutela dei diritti dell'interessato.

9. Come vengono a conoscenza gli interessati della modalità del trattamento dei dati effettuato da DmlAS?

Vengono stilati dei documenti, detti **INFORMATIVA**, dove vengono descritti i dati trattati e le modalità di trattamento. L'**INFORMATIVA** viene adottata sia per le informative riferite all'area Funzionale sia per quella Operativa, l'unica differenza è che, per quanto riguarda l'Area operativa, viene anche specificato il servizio nell'ambito del quale viene espletato il trattamento, al fine di produrre eventuali informative specifiche (*sito internet, newsletter, informative al cliente nel caso di particolari trattamenti dovuti al servizio offerto, ecc.*).

10. Quali sono le modalità per la richiesta del Consenso agli interessati del trattamento dei dati effettuato da DmlAS?

Il Consenso da parte dell'interessato viene raccolto mediante l'apposizione della firma nell'apposito campo dell'Informativa sul trattamento dei dati personali. Questa modalità può subire variazioni nel caso della raccolta del Consenso attraverso il sito dell'organizzazione o relativamente alla gestione dei cookies.





11. È stato nominato un Responsabile Protezione Dati - RPD (Data Protection Officer DPO) in DmlAS?

DMLAS vista la quantità di dati da trattare, la maggior parte dei quali sensibili, ha nominato un Responsabile della Protezione dei dati.

12. Esistono dei documenti che DmlAS ha prodotto per la gestione del GDPR?

DmlAS ha predisposto:

- > il **MANUALE di PROTEZIONE dei DATI PERSONALI** nel quale sono state descritte le modalità con cui si ottempera a quanto stabilito dal Regolamento Europeo n. 2016 / 679 in materia di tutela e protezione dei dati personali;
- > l'**ANALISI DEI PROCESSI (RISK ASSESSMENT)** volta a descrivere le finalità del trattamento dei dati personali, analizzare la natura e la categoria di tali dati nonché degli incaricati e degli interessati e i contesti in cui essi vengono trattati. Vengono inoltre specificati la durata del trattamento, le modalità di conservazione dei dati e la base giuridica di riferimento. Se esistono particolari procedure legate alla conservazione o al trattamento di un dato personale sono esplicitate in tale ambito. In questo documento trovano rilevanza, ai fine **dell'ANALISI DEL RISCHIO**, l'identificazione del tipo di supporto sul quale vengono trattati i dati personali (se sia cioè cartaceo o informatico) e l'eventuale software utilizzato, poiché da ciò potrebbe derivare un rischio differente pur riferendosi allo stesso trattamento.
- > il **REGISTRO ATTIVITÀ DI TRATTAMENTO** nel quale è stato effettuato il censimento e l'analisi dei trattamenti dei dati. Deve essere mantenuto costantemente aggiornato poiché il suo contenuto deve sempre corrispondere all'effettività dei trattamenti posti in essere. Qualsiasi cambiamento, in particolare in ordine alle modalità, finalità, categorie di dati, categorie di interessati, deve essere immediatamente inserito nel Registro, dando conto delle modifiche sopravvenute.





Documento a cura della Direzione,
dell'Ufficio Sistema per la Gestione
della Qualità e dell'Ufficio Tecnico
Progettazione Area Ricerca e Sviluppo



DUEMILAUNO AGENZIA SOCIALE

via Colombara di Vignano 3

34015 Muggia (TS)

tel. 040232331

www.2001agsoc.it