REGOLAMENTO PRIVACY

Data di emissione	*13/02/2019*
Numero revisione	Seconda emissione
Revisione	Aggiornamento processi
Preparato da	Studio SASPI Fieldfisher
Controllato da	**Direzione**
Approvato da	CdA Fondir

FONDIR
IL PRESIDENTE
Riccardo Verità

Indice

1 Introduzione

1.1 Normativa applicabile

Il Regolamento Privacy (di seguito "**Regolamento**") Fondir (Fondo Paritetico Interprofessionale Nazionale per la Formazione Continua dei Dirigenti del Terziario) è adottato in attuazione del "*Regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei Dati personali, nonché alla libera circolazione di tali Dati e che abroga la direttiva 95/46/CE ("General Data Protection Regulation"*, di seguito "**GDPR**").

Il GDPR prevede una disciplina uniforme in tema di *privacy*, valida in tutta l'Unione Europea, ed ha lo scopo di assicurare all'interno della stessa Unione un livello coerente ed elevato di protezione e la rimozione degli ostacoli alla circolazione dei Dati Personali.

Il GDPR è entrato in vigore il 24 maggio 2016 senza necessità di recepimento per mezzo di atti nazionali, ed è applicabile in tutti i Paesi UE a partire dal 25 maggio 2018. L'Autorità Garante per la Protezione dei Dati Personali (di seguito il "**Garante**") ha adottato il 28 aprile 2017 una prima "*Guida all'applicazione del Regolamento europeo in materia di protezione dei Dati personali*", successivamente aggiornata (di seguito "**Guida all'applicazione del GDPR**").

Con il Decreto Legislativo n. 101 del 10 agosto 2018, pubblicato sulla Gazzetta Ufficiale del 4 settembre, entrato in vigore il 19 settembre 2018, l'ordinamento italiana ha recepito ufficialmente le disposizioni del GDPR, introducendo modifiche al D.Lgs 196/03 "*Codice in materia di protezione dei Dati personali*" (di seguito "**Codice Privacy**")..

Il **Regolamento** è quindi redatto tenuto conto delle disposizioni del GDPR nonché delle Linee Guida e dei Provvedimenti del Garante che resteranno in vigore (di seguito la "**Normativa Vigente**")[1].

1.1 Scopo

Lo scopo del presente **Regolamento Privacy** è quello di dare attuazione al GDPR all'interno di Fondir. Pertanto, ai fini della predisposizione del **Regolamento** stesso, il Fondo ha condotto, nel corso di novembre 2017 e a febbraio 2018, un'attività di *Risk Assessment, Gap Analysis & Action Plan* finalizzata all'identificazione dei rischi riconducibili ad una non corretta/adeguata gestione dei dati personali in ottica GDPR, che si è conclusa con la formalizzazione di un report che ha dato evidenza dello stato di adeguamento al Codice *Privacy*, del livello di maturità rispetto al GDPR, dei relativi *gap* riscontrati e del conseguente *action plan* (di seguito il "**Risk Assessment**").

Alla luce degli esiti di tale attività, il Fondo ha pertanto ritenuto, nell'ottica dell'*accountability* prevista dal GDPR e di seguito specificata nel dettaglio, di dotarsi dell'organizzazione *privacy* di seguito descritta.

[1]Il Regolamento potrebbe subire modifiche a seguito di eventuali ed ulteriori linee guida attuative del GDPR o della suddetta norma di coordinamento.

Inoltre, Fondir ha adottato un set di documenti conformi al GDPR (informative, nomine a responsabili, policies IT, etc.) messi a disposizione dei Destinatari, come di seguito definiti, con le modalità specificate nel prosieguo.

In tal senso il presente **Regolamento** fornisce, altresì, indicazioni in merito alle modalità con cui è disciplinato il Trattamento dei dati personali (come di seguito definito) di Dipendenti, Dirigenti delle aziende iscritte e Fornitori, nonché di altri soggetti eventualmente interessati, da parte del Fondo, ed è pertanto predisposto ad hoc sulla base delle specifiche attività operative di Fondir, come identificate nelle tabelle del paragrafo 5. Il Fondo, pertanto, pone in essere le attività di Trattamento di dati personali nell'ambito del perseguimento dei propri scopi, come risultanti dallo Statuto, e nei limiti e secondo le regole previste nella presente Regolamento e nei relativi allegati.

1.2 Destinatari e conseguenze in caso di mancato rispetto del Regolamento Privacy

Le regole e istruzioni contenute nel presente Regolamento sono rivolte a tutti i dipendenti, lavoratori somministrati, eventuali stagisti e collaboratori a qualsiasi titolo del Fondo.

A tal fine si considerano:

- Dipendente/i: un dipendente, un candidato o un precedente dipendente del Fondo, inclusi i lavoratori temporanei che hanno prestato attività lavorativa sotto la diretta supervisione del Fondo (quali, a titolo esemplificativo, tirocinanti, somministrati, distaccati). La presente definizione non include i consulenti che prestano la propria attività presso Fondir, né i dipendenti di soggetti terzi che forniscono servizi in favore del Fondo.
- Collaboratore/i: soggetti che collaborano con Fondir, a prescindere dal rapporto contrattuale (es. agenti non dipendenti, consulenti, professionisti).

La mancata ottemperanza delle disposizioni contenute nel Regolamento Privacy stesso potrà determinare l'applicazione da parte di Fondir di misure restrittive, in merito alle attività di trattamento dati svolte dal Dipendente o Collaboratore, considerate appropriate da quest'ultima, nonché l'applicazione da parte dello stesso:

- dei provvedimenti disciplinari a carico dei Dipendenti previsti dal contratto collettivo nazionale di lavoro;
- della risoluzione del contratto e delle azioni civili e penali stabilite dalla legge, nei confronti dei Collaboratori.

Inoltre, l'inosservanza delle regole previste dal Regolamento Privacy comporta l'applicazione delle misure sanzionatorie contenute nel sistema disciplinare aziendale adottato ai sensi del D.lgs. 231/01 in base alle specifiche modalità ivi previste.

2 Definizioni

Ai fini del presente Regolamento vengono definiti i seguenti termini, la cui definizione non corrisponde necessariamente, per ragioni di maggior chiarezza, a quella indicata dal GDPR.

Dati

- **Dati Personali:** qualsiasi informazione riguardante una persona fisica identificata o identificabile. L'identificazione della persona fisica può avvenire, direttamente o indirettamente, tramite Dati quali: nome, un numero di identificazione, Dati relativi all'ubicazione, elementi caratteristici dell'identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale. Esempio di Dati che identificano direttamente: nome per esteso, indirizzo email, codice fiscale. Esempio di Dati che identificano indirettamente: indirizzi IP, targa di moto/autoveicoli.
- **Categorie Particolari di dati:** dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
- **Dati genetici:** dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione.
- **Dati biometrici:** dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.
- **Dati personali relativi a condanne penali e reati:** informazioni relative a reati attribuiti o a condanne penali subite da una persona fisica, nonché qualsiasi altra informazione ritenuta sensibile ai sensi di legge.
- **Dati:** Dati Personali, Categorie Particolari di dati e dati relativi a condanne penali e reati considerati congiuntamente.

Soggetti

- **Fondir:** il Fondo Paritetico Interprofessionale Nazionale per la Formazione Continua dei Dirigenti del Terziario, anche definito nel seguito come **"Fondo";**
- **Titolare:** la persona (fisica o giuridica), l'autorità pubblica, o qualsiasi altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del Trattamento;
- **Delegato:** figura individuata dal CdA nel Direttore;

- **Responsabile:** la persona (fisica o giuridica), l'autorità pubblica, il servizio o qualsiasi altro organismo, esterno al Fondo, che tratta Dati Personali per conto del Titolare del Trattamento, ai sensi dell'art. 28 del GDPR;
- **Subresponsabile:** la persona (fisica o giuridica) nominata dal Responsabile da parte di un Responsabile per specifiche attività di Trattamento, nel rispetto degli stessi obblighi contrattuali che legano Titolare e Responsabile;
- **Interessato/Interessati:** la persona fisica cui si riferiscono i Dati Personali (ad esempio Dipendenti, Collaboratori, componenti degli organi del Fondo, dipendenti o legali rappresentanti di clienti o Fornitori, personale erogante la formazione, dirigenti partecipanti alle attività formative finanziati dal Fondo, ecc.);
- **DPO:** il Data Protection Officer[2] soggetto nominato dal Fondo in qualità di Responsabile della protezione dei Dati, qualora sussistano i requisiti previsti dall'articolo 37 del GDPR;
- **Amministratore di Sistema:** figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. Vengono considerate tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei Dati, quali gli amministratori di basi di Dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi, secondo la definizione del Provvedimento del Garante del 27 novembre 2008 *"Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema"* (di seguito "**Provvedimento ADS**");
- **Garante Europeo:** l'autorità di sorveglianza indipendente che ha il compito di garantire che le istituzioni e gli organi dell'Unione Europea rispettino il diritto alla protezione dei dati in sede di Trattamento dei Dati Personali e di elaborazione di nuove politiche;
- **Autorità di Controllo:** indica l'autorità pubblica indipendente istituita da uno Stato membro dell'Unione Europea;
- **Garante:** Garante per la protezione dei dati personali. Indica l'Autorità di Controllo italiana;
- **Personale:** si riferisce, indistintamente, a Dipendenti e Collaboratori;

Modalità e strumenti a presidio del Trattamento

- **Regolamento Privacy:** il presente Regolamento, definito nel seguito anche come ***"Regolamento"*** *o* ***"Policy"***.
- **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. Il Trattamento può svolgersi mediante la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante

[2] (individuato nella traduzione italiana del Garante anche "Responsabile Protezione dei Dati")