REGOLAMENTO PRIVACY

Data di emissione	*24/02/2026*
Numero revisione	Terza emissione
Revisione	Aggiornamento processi
Preparato da	DPO - Avv. Paolo Todaro
Controllato da	Direzione
Approvato da	CdA Fondir

FONDIR
Vittorio Cianchi
Presidente

Indice

1 INTRODUZIONE 4

1.1 NORMATIVA APPLICABILE 4
1.1 SCOPO 4
1.2 DESTINATARI E CONSEGUENZE IN CASO DI MANCATO RISPETTO DEL REGOLAMENTO PRIVACY 5

2 DEFINIZIONI 6

DATI 6
SOGGETTI 6
MODALITÀ E STRUMENTI A PRESIDIO DEL TRATTAMENTO 7

3 LE REGOLE GENERALI DEL TRATTAMENTO 8

3.1 IL PRINCIPIO DI *ACCOUNTABILITY* 8
3.2 I PRINCIPI GENERALI DA RISPETTARE NEL TRATTAMENTO DEI DATI 9
3.3 PRINCIPI DA ATTUARE NELL'ORGANIZZAZIONE DEL TITOLARE 10

4 LA *PRIVACY GOVERNANCE* DEL FONDO 11

4.1 IL TITOLARE ED IL DELEGATO PRIVACY 11
4.2 IL RUOLO DEI SOGGETTI "REFERENTI PRIVACY" 12
4.3 I SOGGETTI AUTORIZZATI AL TRATTAMENTO 12
4.4 GLI AMMINISTRATORI DI SISTEMA 13
4.5 IL DATA PROTECTION OFFICER (DPO) 14
4.6 IL RUOLO E LA SCELTA DEI RESPONSABILI 15

5 GLI INTERESSATI 16

5.1 I TRATTAMENTO DEI DATI DEGLI INTERESSATI 17
5.1.1 Dirigenti delle aziende iscritte 17
5.1.2 Esponenti delle aziende iscritte 18
5.1.3 Referenti e docenti degli enti formatori 18
5.1.4 Consulenti delle aziende iscritte 19
5.1.5 Fornitori (persone fisiche, e, per le gare sopra soglia, familiari dei legali rappresentanti delle società fornitrici) 19
5.1.6 Dipendenti, somministrati, candidati, membri degli organi sociali di Fondir 20
5.2 L'INFORMATIVA 21
5.3 IL CONSENSO 23
5.4 I COOKIE 23
5.5 I DIRITTI DELL'INTERESSATO 24
5.5.1 Identificazione dell'Interessato 25
5.5.2 Valutazione della Richiesta 25
5.5.3 Gestione della Richiesta 27
5.5.4 Risposta all'Interessato 28

6 GLI STRUMENTI DI TRATTAMENTO E PROTEZIONE DEI DATI PERSONALI 29

6.1 IL REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO DEL TITOLARE 29
6.2 PROCEDURA DI GESTIONE DEL *DATA BREACH* 30
6.2.1 Segnalazione di un Data Breach *30*
6.2.2 Analisi e valutazione delle segnalazioni *30*
6.2.3 Notificazione al Garante *32*
6.2.4 Comunicazione agli Interessati *32*
6.2.5 Analisi dettagliata *33*
6.3 DATA PROTECTION IMPACT ASSESSMENT (DPIA) 33

7 ALTRI TRATTAMENTI RILEVANTI 36

7.1 VIDEOSORVEGLIANZA 36
7.2 TRATTAMENTO DEI DATI PERSONALI TRAMITE SISTEMI DI INTELLIGENZA ARTIFICIALE (AI) 37
7.2.1 Finalità del trattamento tramite AI *37*
7.2.2 Categorie di dati trattati tramite AI *37*
7.2.3 Modalità di funzionamento dei sistemi AI *37*
7.2.4 Assenza di processi decisionali automatizzati *38*
7.2.5 Misure di sicurezza *38*
7.2.6 Conservazione dei dati *38*
7.2.7 Diritti degli interessati *38*

8 LA GOVERNANCE IT 38

8.1 I PRINCIPI DEL GDPR 38
8.2 IL CODICE DI CONDOTTA PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI DEL FONDO 39
8.3 INDIRIZZI SULL'USO DI SITI E STRUMENTI DI INTELLIGENZA ARTIFICIALE 39

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;

<u>Modalità e strumenti a presidio del Trattamento</u>

- **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")

trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

- **Limitazione di Trattamento:** l'operazione con cui si contrassegnano alcuni Dati Personali trattati, con l'obiettivo di limitarne il Trattamento in futuro.
- **Profilazione:** qualsiasi forma di Trattamento di Dati Personali automatizzato, con cui tali Dati vengano utilizzati per valutare determinati aspetti di una persona fisica, in particolare per analizzare o prevedere il rendimento professionale, la situazione economica, la salute, le preferenze Personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti.
- **Pseudonimizzazione:** una modalità di Trattamento dei Dati Personali effettuata in modo tale che gli stessi Dati non possano più essere attribuiti a un soggetto 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.
- **Consenso dell'Interessato:** 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.
- **Violazione dei Dati Personali ("Data Breach"):** una violazione in termini di sicurezza che comporti accidentalmente o in modo illecito: la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato a Dati Personali trasmessi, conservati o comunque trattati.
- **Registro:** il Registro del Trattamento previsto dal GDPR (articolo 30).
- **DPIA (acronimo di "Data Protection Impact Assessment"):** valutazione d'impatto sulla protezione dei dati previsto dal GDPR (articolo 35).

3 Le regole generali del Trattamento

3.1 Il principio di *accountability*

Il GDPR impone un cambio di prospettiva ed un ruolo maggiormente attivo da parte dei Titolari nel Trattamento dei Dati. In questo senso viene introdotto il concetto di "*accountability*" che si riferisce alla responsabilizzazione del Titolare stesso che deve farsi carico in prima persona di garantire il rispetto delle disposizioni a tutela dei Dati. Il Garante, nella Guida all'applicazione del GDPR, precisa che il Titolare deve attuare dei "comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento". La novità di questo principio consiste nell'attribuzione al Titolare del compito di decidere autonomamente le modalità, le garanzie e i limiti del Trattamento dei Dati Personali nel rispetto della Normativa Vigente.

Queste valutazioni devono essere svolte prima di procedere al Trattamento dei Dati vero e proprio: è necessaria quindi un'analisi preventiva da parte del Titolare che deve sostanziarsi in una serie di attività specifiche e dimostrabili.

A tal proposito il Fondo, come sopra indicato, si è attivato con un *Risk Assessment* per conformare le procedure aziendali al GDPR.

Tutti i Destinatari devono essere pienamente consapevoli delle implicazioni connesse al Trattamento dei Dati e delle regole di cui il Fondo si è dotato al fine garantire una adeguata tutela dei Dati stessi.

Nella gestione e manutenzione del sistema privacy di cui Fondir si è dotato, quest'ultimo ha individuato nella figura del Direttore del Fondo il compito di rivedere periodicamente – e comunque almeno una volta all'anno – lo stato di attuazione della Normativa Vigente, con ausilio del file di Risk Assessment predisposto.
Eventuali successive modifiche delle responsabilità o delle modalità di gestione del suddetto processo sono a cura della Presidenza/Direzione di Fondir.

3.2 I principi generali da rispettare nel trattamento dei Dati

In estrema sintesi, i principi generali posti alla base di qualsiasi Trattamento di Dati Personali, secondo il GDPR, sono:

a) **liceità, correttezza e trasparenza:** i Dati Personali devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'Interessato. Il principio di liceità e correttezza prevede che i Dati di un Interessato possano essere trattati solo se questi: (i) ha espresso il proprio consenso al Trattamento per una o più specifiche finalità, (ii) quando il Trattamento è necessario all'esecuzione di un contratto di cui l'Interessato è parte, (iii) quando il Trattamento è necessario per adempiere un obbligo legale a cui è soggetto il Titolare; (iv) quando il Trattamento è necessario per la salvaguardia degli interessi vitali dell'Interessato o di un'altra persona fisica (v) quando è necessario per l'esecuzione di un compito di interesse pubblico o per il perseguimento del legittimo interesse del Titolare. Inoltre, in omaggio al principio di trasparenza, le modalità con cui sono raccolti e utilizzati i Dati Personali devono essere trasparenti e le informazioni e comunicazioni relative al Trattamento devono esser altresì facilmente accessibili e comprensibili;

b) **limitazione della finalità**: i Dati Personali devono essere raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in un modo che il relativo Trattamento non sia incompatibile con tali finalità. È considerato compatibile con le finalità inziali un ulteriore Trattamento dei Dati Personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici;

c) **minimizzazione dei Dati**: i Dati Personali devo essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati: il Trattamento deve avere ad oggetto solo la quantità dii Dati necessari per eseguire correttamente una determinata attività. Inoltre, i Dati raccolti per uno scopo non possono essere trattati per un altro scopo senza prima acquisire lo specifico consenso da parte dell'Interessato. Il Fondo deve quindi limitare la raccolta, l'archiviazione

e l'utilizzo dei Dati Personali a quelli rilevanti, adeguati e assolutamente necessari per l'esecuzione dello scopo per il quale i dati vengono trattati;

d) **esattezza:** i Dati Personali devono essere esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i Dati inesatti rispetto alle finalità per le quali sono trattati;

e) **limitazione della conservazione:** i Dati Personali devono essere conservati in una forma che consenta l'identificazione degli Interessati per un arco di tempo non superiore al tempo strettamente necessario al conseguimento delle finalità per le quali sono trattati. I Dati Personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal GDPR a tutela dei diritti e delle libertà dell'Interessato;

f) **integrità e riservatezza:** i Dati Personali devono essere trattati in maniera da garantire un'adeguata sicurezza dei Dati Personali, compresa la protezione, mediante misure tecniche e organizzative adeguate per proteggere i Dati stessi da Trattamenti non autorizzati o illeciti, dalla loro perdita o distruzione o dal danno accidentale.

3.3 Principi da attuare nell'organizzazione del Titolare

In base all'art. 25, è necessario rispettare i principi che seguono:

a) ***Privacy by design*** **(o 'fin dalla progettazione'):** tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il Titolare mette in atto 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 GDPR e tutelare i diritti degli Interessati (art. 25, par. 1 GDPR).

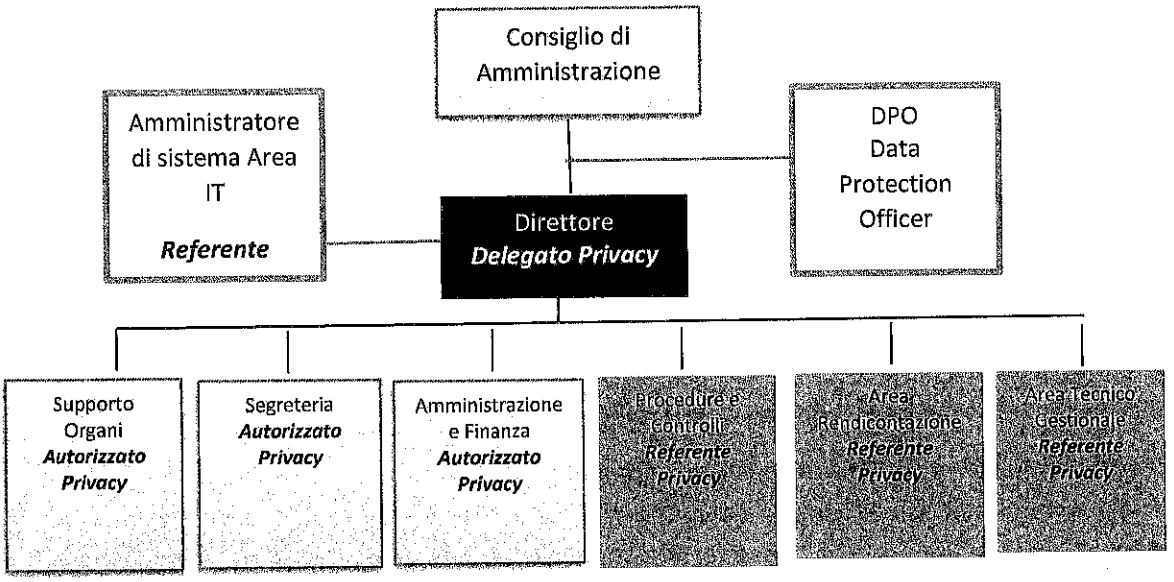
b) ***Privacy by default*** **(o 'per impostazione predefinita'):** il Titolare mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del Trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza un intervento individuale (art. 25, par. 2 GDPR).

In caso di Trattamento effettuato mediante sito web, il soddisfacimento di questi adempimenti richiede un'ampia varietà di interventi, tra i quali ad esempio la configurazione dei sistemi in modo tale che i dati

personali siano eliminati automaticamente alla scadenza del tempo di conservazione specificamente previsto per gli stessi.

4 La *Privacy Governance* del Fondo

Dopo aver svolto l'attività di *Risk Assessment*, Fondir ha ritenuto di dotarsi del seguente organigramma privacy, con ciò intendendosi la struttura organizzativa a presidio dei processi legati alla privacy:



Eventuali successive modifiche operative relative alle responsabilità o alle modalità di gestione del suddetto processo sono a cura della Presidenza/Direzione di Fondir che ne informano il Consiglio di Amministrazione che procede all'approvazione.

4.1 Il Titolare ed il Delegato Privacy

Ai fini dell'applicazione del GDPR, Fondir è Titolare dei Dati trattati nello svolgimento delle proprie attività e contenuti nelle relative banche dati, sia su supporto elettronico che cartaceo.

Il Titolare, identificato nel Consiglio di Amministrazione, ha conferito al Direttore con verbale del Consiglio di Amministrazione del 9 maggio 2018 la delega in materia di privacy, delegandogli i conseguenti poteri necessari all'adempimento degli obblighi previsti dalla Normativa Vigente, compreso il potere di designare e preporre mediante ordini di servizio al trattamento dei Dati uno o più soggetti autorizzati, nonché i Responsabili.

4.2 Il ruolo dei soggetti "Referenti Privacy"

Costituisce una misura organizzativa idonea al rispetto della Normativa Vigente affidare compiti specifici sul Trattamento a figure interne qualificate del Fondo, in ottemperanza al principio di *accountability* cui lo stesso GDPR è permeato.

Il Fondo, nel dare attuazione alla regola di cui all'art. 29 del GDPR, ha ritenuto di modulare le istruzioni da fornire ai soggetti che devono trattare dati sotto la sua responsabilità, in modo da prevedere delle figure intermedie, dotate anche di compiti organizzativi.

Secondo l'organigramma del Fondo, il compito ed il potere di individuare i Referenti Privacy è affidato al Delegato *Privacy* che può anche consultarsi, a tal fine, con il DPO.

In ogni caso, il Delegato *Privacy* - nel presupposto che i Referenti Privacy siano di norma identificabili nei Responsabili e/o nelle figure preposte alla segreteria ed alle aree in cui è funzionalmente articolata l'organizzazione del Fondo - deve comunque assicurarsi che tali soggetti siano in grado di fornire idonee garanzie in termini di esperienza, capacità ed affidabilità circa l'osservanza della normativa vigente e garantire il rispetto delle istruzioni ricevute, ivi compreso il profilo della sicurezza; tale principio e requisito è da considerarsi normalmente esteso anche nei confronti dei dipendenti del Fondo autorizzati al trattamento.

Per formalizzare l'incarico di Referenti Privacy, il Delegato *Privacy* deve utilizzare il *template* di nomina disponibile presso il Fondo adottando un ordine di servizio.

Il documento dovrà essere adattato a seconda dei compiti, coerenti con la propria funzione, che si vogliono affidare al nominando Referente Privacy. Per questa il Delegato Privacy oltre a consultare il DPO, può coinvolge un Referente Privacy che fornirà supporto sia per la redazione della singola nomina che per il conseguente adattamento del documento.

Eventuali successive modifiche operative relative alle responsabilità o alle modalità di gestione del suddetto processo sono a cura della Presidenza/Direzione di Fondir che ne informano il Consiglio di Amministrazione.

4.3 I soggetti Autorizzati al Trattamento

Il GDPR, all'art. 29, precisa che chiunque agisca sotto l'autorità del Titolare e che abbia accesso a Dati non può trattare tali Dati se non è debitamente istruito in tal senso dal Titolare medesimo.

Il Direttore coordinandosi con il responsabile della funzione per la quale l'Autorizzato al Trattamento è destinato ad operare, ha il compito di consegnare formalmente le istruzioni specifiche per il tipo di attività che quest'ultimo dovrà svolgere sui dati.

A tal fine, il Direttore, dovrà utilizzare il *template* di istruzioni disponibile presso il Fondo, le cui istruzioni dovranno essere riportate in un Ordine di Servizio.

L'ambito del Trattamento dell'Autorizzato al Trattamento viene individuato sulla base delle mansioni e degli applicativi a cui deve avere accesso lo stesso.

I profili di autorizzazione – soprattutto in caso di cambiamento della mansione – verranno creati dalla funzione IT previa autorizzazione del Responsabile dell'area a cui viene assegnato l'Autorizzato al Trattamento. Conseguentemente verranno assegnate le credenziali di autenticazione.

Le istruzioni vengono consegnate unitamente al *Welcome Kit (Regolamento Privacy, Codice di condotta degli strumenti informatici, nomina autorizzato/referente al trattamento dei dati, informativa privacy dipendenti).*

Eventuali successive modifiche operative relative alle responsabilità o alle modalità di gestione del suddetto processo sono a cura della Presidenza/Direzione.

4.4 Gli Amministratori di Sistema

La figura di Amministratore di Sistema è contenuta nel Provvedimento ADS e il Fondo ha ritenuto di mantenerla, unitamente alle prescrizioni previste dal medesimo Provvedimento ADS (quali ad esempio la registrazione dei *file Log,* ecc.). Il Fondo ha infatti valutato che tale nomina contribuisse ad una corretta organizzazione dei ruoli privacy interna e costituisse, altresì, una adeguata misura di tutela dei Dati che la stessa tratta nello svolgimento della propria attività.

La facoltà di nominare gli Amministratori di sistema è attribuita al Direttore che ha individuato il Consulente IT come ADS. La nomina viene consegnata unitamente alla lettera di incarico del Consulente e alla Nomina di Responsabile del Trattamento.

Il Direttore, nel formalizzare la predetta nomina, provvede a far sottoscrivere all'ADS un apposito atto, predisposto eventualmente anche con il supporto del DPO.

Qualora le attività di Amministratore di Sistema siano svolte da una società esterna, non sarà necessario procedere a tale nomina. In tal caso si deve far riferimento a quanto previsto in seguito a proposito di Nomina dei Responsabili.

L'operato degli Amministratori di Sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte del Titolare, anche eventualmente avvalendosi di un consulente esterno.

Devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (*access log*) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste.

Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.

Eventuali successive modifiche operative relative alle responsabilità o alle modalità di gestione del suddetto processo sono a cura del Direttore.

4.5 Il Data Protection Officer (DPO)

Il GDPR individua una nuova figura nell'ambito del governo della privacy (articoli 37-39 del GDPR) che dovrà:

- informare e fornire consulenza al Titolare e al Responsabile in merito agli obblighi derivanti dalla Normativa Vigente;
- sorvegliare l'osservanza del GDPR da parte del Titolare e dei Responsabili, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa al Trattamento;
- fornire su richiesta pareri in merito alla valutazione d'impatto e sorvegliarne lo svolgimento;
- cooperare con il Garante fungendo, tra le altre cose, da punto di contatto per questioni connesse al Trattamento, effettuando consultazioni di ogni tipo, con particolare riguardo e attenzione ad un'eventuale attività di consultazione preventiva;
- sovraintendere alla tenuta e al costante aggiornamento di un registro delle attività del trattamento svolte sotto la responsabilità di Fondir, sia in qualità di titolare che di responsabile del trattamento, ove ne ricorrano i presupposti di cui alla Normativa applicabile.

La funzione del DPO può essere ricoperta da un soggetto con conoscenze specialistiche della Normativa Vigente e delle prassi in materia di protezione Dati. Il DPO deve essere scelto in base alle sue qualità professionali ed alla sua preparazione in ambito di Trattamento Dati, sia sul piano teorico che su quello pratico. Questa figura può essere scelta tra i Dipendenti che non siano coinvolti in attività di Trattamento dei Dati del Fondo oppure può essere un libero professionista, esterno e autonomo, incaricato in base a un contratto di servizi. Il GDPR prevede che il DPO debba essere obbligatoriamente nominato dal Titolare in tre occasioni:

1) quando il Trattamento è effettuato da un'autorità pubblica o da un organismo pubblico (ad eccezione delle autorità giurisdizionali nell'esercizio delle loro funzioni);
2) quando le attività principali del Titolare o del Responsabile consistono in Trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli Interessati su larga scala.
3) quando le attività principali del Titolare o del Responsabile consistono nel Trattamento su larga scala, di categorie particolari di dati personali (art. 9) o di dati relativi a condanne penali e reati di cui all'articolo 10 GDPR, ossia di Dati Sensibili e Dati Giudiziari.

In tutti gli altri casi la nomina del DPO è comunque facoltativa da parte del Titolare.

Fondir rientra tra quei soggetti che, pur avendo assunto la forma di un ente privatistico, possono essere qualificati come organismi di diritto pubblico, soddisfando tutti e tre i requisiti normativamente richiesti[3], e pertanto esso risulta tenuto al rispetto dell'obbligo di nomina del DPO ai sensi dell'art. 37, comma 1, lett. a) GDPR.
In ogni caso, in base al principio della *accountability*, Fondir ritiene comunque opportuno provvedere alla nomina di un DPO.
Il Fondo, quale Titolare, supporta il DPO nell'esecuzione dei propri compiti, condividendo con lo stesso i fabbisogni e le conseguenti risorse necessarie. Inoltre, esso coinvolge tempestivamente e adeguatamente il DPO nei casi di necessità.
Il DPO svolge la propria attività in assoluta autonomia ed indipendenza, senza porre in essere mansioni o compiti in conflitto di interessi, neanche indiretto o potenziale, con le funzioni proprie richieste o svolte per altro incarico o funzione.
In via meramente esemplificativa il DPO dovrà essere coinvolto nelle iniziative relative al trattamento dati dei dirigenti delle aziende iscritte al Fondo e nei nuovi processi riguardanti i dati dei Dipendenti.
Eventuali successive modifiche operative relative alle responsabilità o alle modalità di gestione del suddetto processo sono a cura della Presidenza/Direzione.

4.6 Il ruolo e la scelta dei Responsabili

Qualora il Trattamento debba essere effettuato per conto del Fondo da un soggetto ad esso terzo è necessario procedere a nominare quest'ultimo Responsabile ai sensi dell'art. 28 del GDPR.

Questi soggetti - in sede di instaurazione del rapporto con Fondir - devono espressamente impegnarsi ad osservare la normativa vigente, nonché offrire garanzie di esperienza, capacità ed affidabilità in tal senso, come pure circa l'affidabilità sull'ottemperanza alle istruzioni ricevute.

Il Referente Privacy, di volta in volta interessato, dovrà comunicare la necessità di nominare Responsabile un fornitore al Responsabile della funzione Procedure e Controlli (o altro Referente Privacy responsabile della procedura di approvvigionamenti), il quale dovrà verificare, sulla base delle attività che saranno affidate al fornitore, e prima dell'attivazione del processo di gara, se quest'ultimo tratterà Dati per conto di Fondir.

Qualora l'esito della valutazione sia positivo, sarà necessaria, ad aggiudicazione del servizio avvenuta, la sottoscrizione da parte del fornitore di un atto di "Nomina a Responsabile del Trattamento" che dovrà essere allegato al contratto e/o all'ordine di acquisto e, in ogni caso, archiviato a cura della funzione Procedure e Controlli.

[3] La Direttiva 2003/98/UE (come modificata dalla direttiva 2013/37/UE) prevede che, ai fini della stessa, si intende per «organismo di diritto pubblico», "qualsiasi organismo: a) istituito per soddisfare specificatamente bisogni d'interesse generale aventi carattere non industriale o commerciale; e b) dotato di personalità giuridica; e c) lo cui attività è finanziata in modo maggioritario dallo Stato, da autorità regionali o locali o da altri organismi di diritto pubblico, oppure la cui gestione è soggetta al controllo di questi ultimi, oppure il cui organo d'amministrazione, di direzione o di vigilanza è costituito da membri più della metà dei quali è designato dallo Stato, da autorità regionali o locali o da altri organismi di diritto pubblico".

Per formalizzare la nomina dovrà essere utilizzato il *template* di nomina disponibile presso il Fondo.

Il Direttore del Fondo fornirà supporto sia per la redazione della singola nomina che per il conseguente adattamento del documento.

Se del caso, potrà essere coinvolto il DPO.

Inoltre, il fornitore, consulente o collaboratore che tratterrà dati personali per conto del Fondo, dovrà essere sottoposto ad Audit in data successiva alla stipula del contratto, al fine di assicurare l'adeguatezza delle misure tecniche e organizzative volte a proteggere i dati personali. L'attività di audit, sarà gestita dal Responsabile di Area o funzione di riferimento, e potrà essere svolta eventualmente anche con il supporto di un Auditor esterno specializzato e nelle modalità ritenute più opportuno da Fondir (ad es. tramite compilazione di *checklist* da parte del fornitore circa l'effettiva implementazione delle misure tecniche-organizzative, acquisizione di precedenti audit svolti da altri terzi presso il fornitore, esecuzione di audit *on-field* presso le sedi operative del fornitore), sulla base di una valutazione del livello di rischio privacy correlato con l'attività di trattamento che sarà affidata al fornitore. Nell'eventualità in cui i risultati dell'audit rilevino gravi inidoneità con riferimento alle misure tecniche e organizzative adottate dal potenziale fornitore, non sanabili immediatamente a cura di quest'ultimo, questi dovrà essere escluso dal processo di gara oppure (in caso di contratto già stipulato) il Fondo dovrà procedere con la risoluzione di diritto del rapporto.

Eventuali successive modifiche operative relative alle responsabilità o alle modalità di gestione del suddetto processo sono a cura della Presidenza/Direzione.

5 Gli Interessati

Il GDPR, all'art. 6, prevede che il Trattamento è lecito ove sussista una delle seguenti condizioni:

a. l'Interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;

b. il trattamento è necessario all'esecuzione di un contratto di cui l'Interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;

c. il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il Titolare;

d. il trattamento è necessario per la salvaguardia degli interessi vitali dell'Interessato o di un'altra persona fisica;

e. il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare;

f. il trattamento è necessario per il perseguimento del legittimo interesse del Titolare o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

Sulla base delle proprie attività, il Fondo ha individuato quali basi giuridiche del Trattamento tre categorie illustrate nelle tabelle del successivo paragrafo (contratto, consenso e adempimento normativo).

Per eventuali trattamenti fondati su differenti basi giuridiche, come ad esempio sul legittimo interesse il Fondo provvederà ad individuare espressamente tale ulteriore base giuridica.

Fondir, per i trattamenti basati su un legittimo interesse, effettuerà un bilanciamento secondo il seguente schema:

a. Il Fondo ha un legittimo interesse ad effettuare un tipo di Trattamento, anche eventualmente in quanto funzionale all'assolvimento delle proprie finalità istituzionali, così come stabilite dalla vigente normativa, dallo statuto, dal regolamento del Fondo e dalle disposizioni emanate dalle Autorità vigilanti sul Fondo stesso;

b. il Trattamento è necessario per perseguire il proprio legittimo interesse;

c. l'interesse del Fondo non prevale sugli interessi, i diritti fondamentali e le libertà degli Interessati.

A titolo esemplificativo, gli Interessati del Trattamento dei Dati di cui Fondir è Titolare possono essere inquadrati nelle seguenti categorie:

- Dirigenti delle aziende iscritte
- Esponenti delle aziende iscritte (Legale Rappresentante, referenti interni)
- Referenti e docenti degli enti formatori
- Consulenti delle aziende iscritte
- Fornitori (persone fisiche)
- Dipendenti, somministrati, candidati, membri degli organi sociali di Fondir

5.1 I Trattamento dei dati degli Interessati

5.1.1 Dirigenti delle aziende iscritte

Dirigenti								
Dati Trattati		Finalità				Base giuridica		
		Contrattuale	Profilazione	Marketing	Obblighi normativi	Contratto	Consenso	Normativa
Anagrafici	SI	✓			✓	✓		✓
Di contatto	NO							
Sensibili	SI	✓			✓	✓		✓
Di profilazione	NO							
Di geolocalizzazione	NO							
Biometrici	NO							
Genetici	NO							

Giudiziari	NO							
Bancari	NO							
Immagine	NO							
Altro								

5.1.2 Esponenti delle aziende iscritte

Esponenti delle aziende iscritte								
Dati Trattati		Finalità				Base giuridica		
		Contrattuale	Profilazione	Marketing	Obblighi normativi	Contratto	Consenso	Normativa
Anagrafici	SI	✓				✓		
Di contatto	SI	✓				✓		
Sensibili	NO							
Di profilazione	NO							
Di geolocalizzazione	NO							
Biometrici	NO							
Genetici	NO							
Giudiziari	NO							
Bancari	NO							
Immagine	NO							
Altro								

5.1.3 Referenti e docenti degli enti formatori

Referenti e docenti degli enti formatori								
Dati Trattati		Finalità				Base giuridica		
		Contrattuale	Profilazione	Marketing	Obblighi normativi	Contratto	Consenso	Normativa
Anagrafici	SI	✓				✓		
Di contatto	SI	✓				✓		
Sensibili	NO							
Di profilazione	NO							
Di geolocalizzazione	NO							
Biometrici	NO							
Genetici	NO							
Giudiziari	NO							
Bancari	NO							

Immagine	NO							
Altro								

5.1.4 Consulenti delle aziende iscritte

Consulenti delle aziende iscritte								
Dati Trattati		Finalità				Base giuridica		
		Contrattuale	Profilazione	Marketing	Obblighi normativi	Contratto	Consenso	Normativa
Anagrafici	SI	✓				✓		
Di contatto	SI	✓				✓		
Sensibili	NO							
Di profilazione	NO							
Di geolocalizzazione	NO							
Biometrici	NO							
Genetici	NO							
Giudiziari	NO							
Bancari	NO							
Immagine	NO							
Altro								

5.1.5 Fornitori (persone fisiche, e, per le gare sopra soglia, familiari dei legali rappresentanti delle società fornitrici)

Fornitori (persone fisiche)								
Dati Trattati		Finalità				Base giuridica		
		Contrattuale	Profilazione	Marketing	Obblighi normativi	Contratto	Consenso	Normativa
Anagrafici	SI	✓			✓	✓		✓
Di contatto	SI	✓				✓		
Sensibili	NO							
Di profilazione	NO							
Di geolocalizzazione	NO							
Biometrici	NO							
Genetici	NO							
Giudiziari	SI	✓						✓
Bancari	SI	✓				✓		
Immagine	NO							
Altro	SI	✓						

5.1.6 Dipendenti, somministrati, candidati, membri degli organi sociali di Fondir

Dipendenti, somministrati, candidati, membri degli organi sociali di Fondir								
Dati Trattati		Finalità				Base giuridica		
		Contrattuale	Profilazione	Marketing	Obblighi normativi	Contratto	Consenso	Normativa
Anagrafici	SI	✓			✓	✓		✓
Di contatto	SI	✓				✓		
Sensibili	SI	✓			✓	✓		✓
Di profilazione	NO							
Di geolocalizzazione	NO							
Biometrici	NO							
Genetici	NO							
Giudiziari	SI	✓						
Bancari	SI	✓				✓		
Immagine	NO							
Altro	Si	✓						

Eventuali successive modifiche operative rispetto all'aggiornamento delle predette tabelle in funzione delle attività di trattamento dati poste in essere dal Fondo sono a cura della Presidenza/Direzione.

Il Fondo, inoltre, ha individuato, per ciascuna categoria di Dati, in relazione a ciascuna finalità, i relativi tempi massimi di conservazione consentiti.

I Dati Personali possono, talvolta, essere trattati contestualmente per plurime finalità che possono comportare differenti tempi di conservazione dei Dati stessi. In tale caso, i Dati Personali potranno essere conservati per il tempo necessario al conseguimento della finalità che prevede il trattamento per il periodo più lungo, fermo restando che non sarà più possibile trattarli per la finalità il cui termine di conservazione sia scaduto.

Di seguito si riportano in forma schematica le regole di cancellazione applicate alle singole aree (finalità) di trattamento.

Finalità	Categoria dei dati	Termine iniziale del periodo di conservazione	Periodo di conservazione
Gestione operativa dei piani formativi (emissione bandi, valutazione, rendicontazione, rapporti con vari interlocutori)	**Consulenti delle aziende iscritte, Referenti e docenti degli enti formatori, Esponenti delle aziende iscritte:** Dati di contatti, dati anagrafici	Data di chiusura dell'esercizio finanziario di riferimento di ogni singolo Piano formativo (circolare ANPAL)	10 anni
Gestione operativa dei piani formativi (emissione bandi, valutazione, rendicontazione,	**Dirigenti:** dati anagrafici, dati sensibili	Data di chiusura dell'esercizio finanziario di riferimento di ogni singolo	10 anni

Finalità	Categoria dei dati	Termine iniziale del periodo di conservazione	Periodo di conservazione
rapporti con vari interlocutori)		Piano formativo (circolare ANPAL)	
Gestione delle gare e dei rapporti contrattuali con fornitori	**Fornitori:** dati anagrafici, dati di contatto, dati giudiziari, dati bancari, dati giudiziari, altri dati riportati nei CV/profili di professionisti	Data di chiusura del contratto	10 anni
Assunzione	**Candidati:** dati anagrafici, dati di contatto, dati giudiziari, altri dati riportati nel CV	Ricezione del CV	6 mesi
Gestione amministrativa e organizzativa del rapporto di lavoro	**Dipendenti:** dati anagrafici, dati di contatto, dati bancari, dati relativi alla salute, altri dati contrattuali, altri dati relativi a formazione e performance	Cessazione del rapporto di lavoro	20 anni
Gestione degli organi sociali	Membri degli organi sociali: dati anagrafici, dati di contatto	Cessazione dell'incarico	10 anni
Attività di Marketing	**Esponenti delle aziende iscritte:** Dati di contatti, dati anagrafici	Data di registrazione dei dati personali	24 mesi
Obblighi normativi legali e fiscali	**Varie categorie di interessati:** dati anagrafici, altri dati fiscalmente rilevanti	Dati di registrazione dei documenti	10 anni

Eventuali successive modifiche operative relative alle responsabilità o alle modalità di gestione del suddetto processo, con particolare riferimento alle tempistiche di conservazione dei dati suindicate, sono a cura della Presidenza/Direzione.

5.2 L'informativa

L'informativa deve essere fornita preventivamente rispetto al Trattamento dei Dati ed essere indirizzata/fornita specificamente a ciascuna categoria di Soggetti Interessati.

I modelli di informativa da utilizzare a seconda delle circostanze sono disponibili presso ciascun Referente Privacy, a seconda del proprio ruolo.

Fondir ha individuato le seguenti tipologie di soggetti interessati del trattamento al quale fornire la propria informativa privacy. In relazione a ciascuna categoria di interessati sono indicate nella seguente tabella anche le occasioni nel corso delle quali vengono raccolti i Dati degli Interessati e le modalità di rilascio dell'informativa. Le relative informative potranno anche riguardare due o più soggetti interessati indicati nella seguente tabella, e rilasciate agli stessi con differenti modalità di trasmissione.

Soggetti interessati	Occasione di trasmissione Informativa al Soggetto Interessato	Modalità di trasmissione Informativa al Soggetto Interessato
Dirigenti che partecipano agli eventi formativi finanziati dal Fondo	• contatto con i responsabili del Fondo • tramite l'azienda iscritta	• Sito Fondir • invio e-mail
Esponenti delle aziende iscritte (Legale Rappresentante, referenti interni)	• Invio on-line formulario di presentazione piano formativo • partecipazione eventi • altra occasione di primo contatto con Interessato	• Sito Fondir
Referenti, consulenti e docenti degli enti formatori	• iscrizione bacheca • altra occasione di primo contatto con l'Interessato	• Sito Fondir • invio e-mail
Consulenti delle aziende iscritte	• primo contatto con l'Interessato	• Sito Fondir • invio e-mail
Fornitori (persone fisiche)	• trasmissione documenti per partecipazione a gare	• invio e-mail • sito Fondir
Dipendenti, somministrati, candidati, membri degli organi sociali di Fondir	• primo contatto con candidati • assunzione / incarico	• invio e-mail / cartaceo

Con specifico riferimento ai Dati Personali dei Dipendenti e Collaboratori, il Fondo può trattare, tra gli altri, dati anagrafici, codice fiscale, dati retributivi, eventuali coordinate bancarie. Può accadere inoltre che, nell'adempimento di specifici obblighi relativi alla gestione del rapporto di lavoro/collaborazione (nei limiti in cui sia applicabile), il Fondo venga in possesso di Categorie particolari di dati e cioè quelli da cui possono eventualmente desumersi, fra l'altro, l'origine razziale ed etnica, l'adesione a partiti, sindacati, nonché un generale stato di salute (ad esempio, certificati di malattia e infortunio; certificati di gravidanza; appartenenza alle c.d. categorie protette; esiti di visite mediche effettuate ai sensi di legge e di contratto, *etc.*). Questi ultimi possono formare oggetto di Trattamento senza consenso.
I soggetti autorizzati al trattamento dati nell'ambito della funzione Amministrazione e Finanza del Fondo sono tenuti alla costituzione dell'archivio delle informative dei Dipendenti, ai fini di permettere in qualsiasi momento le opportune verifiche e al riguardo provvede il giorno stesso dell'assunzione a consegnare al neoassunto l'informativa per i Dipendenti che l'Interessato deve riconsegnare firmata per presa visione; l'informativa sottoscritta deve essere inserita nella cartella del Dipendente.

Eventuali successive modifiche operative relative alle responsabilità o alle modalità di gestione del suddetto processo sono a cura della Presidenza/Direzione.

5.3 Il consenso

Il consenso dell'Interessato al Trattamento dei suoi Dati Personali deve essere richiesto ogni qualvolta non trovi applicazione una delle altre basi giuridiche previste dal GDPR.

Nell'ambito delle proprie attività, il Fondo svolge attività di promozione dei propri servizi mediante inviti via e-mail ad eventi cui possono partecipare alcuni degli Interessati sopra individuati. Sebbene tale attività di promozione possa rientrare nella categoria del marketing (per la quale di norma occorre il preventivo consenso), l'attività di promozione svolta dal Fondo mediante la sola posta elettronica può essere inquadrata c.d. "*soft spam*" in relazione al quale il Garante ha chiarito che: "*se il titolare del trattamento utilizza, a fini di vendita diretta di propri prodotti o servizi, le coordinate di posta elettronica fornite dall'interessato nel contesto della vendita di un prodotto o di un servizio, può non richiedere il consenso dell'interessato. Ciò, però, sempre che si tratti di servizi analoghi a quelli oggetto della vendita e che l'interessato, adeguatamente informato, non rifiuti tale uso*" (Linee guida del Garante Privacy in materia di attività promozionale e contrasto allo spam del 4 luglio 2013).

In altri casi di trattamento, Fondir potrebbe essere tenuta a richiedere il consenso agli interessati, come ad esempio per le seguenti finalità:

- marketing (diverso dal c.d. "Soft Spam");
- marketing profilato;
- trattamento immagini;
- comunicazione a terzi per finalità di marketing, ecc.

In tali casi, i consensi raccolti da Fondir saranno custoditi ed archiviati in una apposita banca dati gestita dalla Segreteria. Gli inserimenti in banca dati dovranno evidenziare eventuali modifiche/revoche del medesimo consenso. I consensi rilasciati in forma cartacea saranno inseriti da parte di un incaricato nella medesima banca dati informatica.

Eventuali successive modifiche operative relative alle responsabilità o alle modalità di gestione del suddetto processo sono a cura della Presidenza/Direzione.

5.4 I cookie

I *cookie* sono dei file utilizzati dai *server* per poter riconoscere i *browser* durante comunicazioni con il protocollo HTTP usato per la navigazione *web*. Tale riconoscimento permette di: realizzare meccanismi di autenticazione, usati ad esempio per i *login*; memorizzare dati utili alla sessione di navigazione, come le preferenze sull'aspetto grafico o linguistico del sito; associare dati memorizzati dal *server*, ad esempio il contenuto del carrello di un negozio elettronico; tracciare la navigazione dell'utente, ad esempio per fini statistici o pubblicitari.

Secondo l'Informativa Cookie presente sul sito web del Fondo, durante la navigazione del sito stesso vengono acquisiti i seguenti tipi di cookies: tecnici/funzionali, di statistica di prima parte, di statistica di terza parte. Gli utenti del sito devono essere informati con un linguaggio chiaro e semplice in merito a chi riceve i loro dati e come sono usati, come previsto nella relativa informativa *cookie*.

I *cookie* devono essere trattati come Dati Personali e pertanto non possono essere tracciati o usati prima che l'utente abbia fornito un consenso esplicito, ad eccezione di quelli meramente tecnici, per i quali non occorre il consenso. È necessario altresì mantenere traccia di ogni consenso – ove richiesto – al trattamento dei *cookies*. La revoca del consenso deve essere facile da effettuare, in maniera simile alla prestazione del consenso medesimo, in qualsiasi momento.

Eventuali successive modifiche operative relative alle responsabilità o alle modalità di gestione del suddetto processo relativo all'utilizzo dei cookie sono a cura della Presidenza/Direzione.

5.5 I diritti dell'Interessato

Il GDPR si prefigge di restituire agli Interessati il controllo dei propri Dati. Affinché gli stessi possano verificare l'esattezza e la liceità del trattamento dei propri Dati, Fondir ha previsto apposite modalità di invio di richieste di informazioni, mediante le quali il Fondo garantisce che le persone fisiche possano esercitare i loro diritti.

Il presente capitolo regolamenta la gestione delle richieste pervenute dagli Interessati inerenti ai Dati (di seguito anche "**Richieste**"), come definiti al paragrafo successivo, con riferimento a:

- accesso ai Dati;
- portabilità dei Dati;
- cancellazione dei Dati;
- rettifica dei Dati;
- revoca del consenso;
- limitazione del trattamento dei Dati;
- opposizione al trattamento dei Dati.

Le Richieste pervenute dagli Interessati vengono gestite attraverso un processo che si articola nelle seguenti quattro fasi:

1) identificazione dell'Interessato;
2) valutazione della Richiesta;
3) gestione della Richiesta;
4) risposta all'Interessato.

In ogni caso il riscontro alla Richiesta deve essere fornito all'Interessato senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della Richiesta stessa. Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle Richieste. In tal caso l'Interessato dovrà essere avvisato di tale proroga, e dei motivi del ritardo, entro un mese dal ricevimento della Richiesta.

5.5.1 Identificazione dell'Interessato

Modalità di ricezione richiesta:

1) contatto telefonico del Fondo;
2) indirizzo PEC o email;
3) posta cartacea.

Tutti coloro che, nell'esecuzione delle rispettive mansioni, sono deputati ad accedere ai suddetti canali informativi, nel momento in cui si avvedono della natura della comunicazione, tempestivamente e comunque entro le 24 ore, inoltrano la richiesta alla Segreteria che provvede a protocollare la richiesta.

La Segreteria al ricevimento della Richiesta identifica l'Interessato avvalendosi dei Dati presenti nella stessa ed esegue un confronto con quelli eventualmente in suo possesso nelle banche dati del Fondo o in archivi cartacei.

Qualora i Dati acquisiti dall'Interessato non fossero sufficienti ai fini dell'identificazione, la Segreteria richiede maggiori dettagli allo stesso. La Segreteria, al fine di certificare l'identità dell'Interessato, richiede una o più informazioni non conosciute al pubblico che permettono di identificare l'Interessato (ID cliente, Azienda di appartenenza, ecc.). Nel caso in cui la Segreteria incontri delle difficoltà in tale processo, può adottare delle soluzioni alternative come l'invio di un codice di conferma al numero di telefono in suo possesso, oppure una videochiamata o provvedere alla raccolta di risposte via email. Non sarà necessario chiedere ulteriori chiarimenti nel caso in cui la richiesta pervenga da avvocati, Autorità ecc., in presenza di elementi ragionevolmente certi in merito alla provenienza della richiesta (ad esempio carta intestata/PEC dell'avvocato o dell'Autorità).

Se l'Interessato non è chiaramente identificabile la Segreteria comunica allo stesso l'impossibilità a procedere rigettando così la richiesta, altrimenti l'iter prosegue regolarmente.

Se la ricerca nel sistema non ha prodotto risultati, la Segreteria comunica quanto emerso all'Interessato portando alla chiusura del processo; al contrario, ove il nominativo sia presente nel sistema l'iter prosegue regolarmente.

La Segreteria, per garantire la tracciabilità delle attività effettuate, registra la ricezione della Richiesta su un apposito file Excel con contestuale apertura di un caso.

5.5.2 Valutazione della Richiesta

La Segreteria, anche con il supporto del Direttore, analizza la Richiesta e individua la tipologia della stessa (accesso, portabilità, cancellazione, rettifica, revoca del consenso, limitazione del trattamento dei Dati, opposizione al trattamento dei Dati). La Segreteria, prima di gestire la Richiesta pervenuta, verifica l'esistenza di altre Richieste in corso di elaborazione nel periodo o la presenza di Richieste identiche già presentate dal medesimo Interessato che potrebbero ostacolare la gestione dell'ultima; in questo caso la Segreteria comunica all'Interessato l'impossibilità a procedere portando al rigetto della stessa.

Il processo prosegue regolarmente se la richiesta pervenuta risulta essere diversa o presenta delle finalità differenti rispetto alle richieste in corso di elaborazione.

La Segreteria, dopo aver definito chiaramente il contenuto della richiesta, valuta la fattibilità di quanto richiesto, secondo il seguente schema:

Tipologia di Richiesta	Casi in cui il diritto è esercitabile
Accesso ai Dati	Tutti i casi
Portabilità dei Dati	**a)** il trattamento si basa su un consenso o su un contratto oppure: **b)** è effettuato con mezzi automatizzati.
Cancellazione dei Dati	**a)** i Dati non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati; **b)** l'Interessato revoca il consenso su cui si basa il Trattamento, se non sussiste altro fondamento giuridico per il Trattamento; **c)** l'interessato si oppone al Trattamento basato sul legittimo interesse del Fondo, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento effettuato per marketing diretto; **d)** i Dati sono stati trattati illecitamente; **e)** i Dati devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento. **Il Fondo può non accogliere la richiesta di cancellazione, se** **a)** il trattamento è necessario ai fini dell'esercizio dei diritti di libertà d'espressione e di informazione; **b)** il trattamento è necessario per adempiere ad un obbligo di legge, oppure è basato su un altro presupposto giuridico diverso dal consenso o dall'interesse legittimo, o comunque finalizzato all'assolvimento delle proprie finalità istituzionali o alle disposizioni emanate da Autorità vigilanti; **c)** il trattamento è necessario per promuovere un diritto o per coltivare la difesa in un giudizio.

Rettifica dei Dati	Tutti i casi, ad eccezione dei dati che non posso essere rettificati, ad esempio immagini o file di log, o altre tipologie di dati generati da sistemi informatici e non forniti dall'Interessato
Revoca del consenso	Tutti i casi di trattamenti basati sul consenso dell'Interessato
Limitazione del trattamento dei Dati	**a)** l'Interessato contesta l'esattezza dei Dati, e chiede la limitazione del trattamento per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali Dati; **b)** il trattamento è illecito e l'Interessato si è opposto alla cancellazione dei Dati e ha chiesto invece che ne sia limitato l'utilizzo; **c)** benché Fondir non ne abbia più bisogno ai fini del trattamento, i Dati sono necessari all'Interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria; **d)** l'Interessato si è opposto al trattamento basato sul legittimo interesse e, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'Interessato, ha chiesto la limitazione del trattamento.
Opposizione al trattamento dei Dati	Tutti i casi, ad eccezione dei trattamenti basati su di un legittimo interesse del Titolare, che prevale sugli interessi, sui diritti e sulle libertà dell'Interessato, necessari per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

5.5.3 Gestione della Richiesta

Una volta confermata la possibilità di accogliere la Richiesta, la Segreteria inoltra la Richiesta pervenuta al Responsabile della Funzione interessata (identificato a seconda della categoria dell'Interessato e della tipologia di Richiesta) che provvede a dare seguito alla Richiesta entro il termine previsto.

Qualora i Dati dell'Interessato fossero comunicati ai fornitori nominati Responsabili del Trattamento, il la Segreteria inoltra ai suddetti fornitori la richiesta ricevuta, entro 2 giorni dalla sua ricezione ai fini della sua evasione.

La Segreteria annota ogni inoltro della Richiesta a soggetti interni ed esterni sul file Excel e monitora la tempestività della risposta. Infine, sollecita in caso di ritardi.

Il Responsabile della Funzione interessata e/o i fornitori esterni inviano l'estratto dei dati dalle banche dati rilevanti (per Richieste di accesso/portabilità) o la conferma di avvenuta esecuzione della Richiesta (rettifica, cancellazione, limitazione/terminazione del trattamento) alla Segreteria.

In caso di accesso/portabilità, la Segreteria, anche con il supporto del Direttore, verifica quanto estratto ed ottenuto dai fornitori nominati al fine di assicurare la correttezza, accuratezza e completezza dei Dati e la corrispondenza con quanto richiesto dall'Interessato.

5.5.4 Risposta all'Interessato

La Segreteria predispone, con il supporto del Direttore, la lettera di risposta all'Interessato e la invia tramite email, senza ingiustificato ritardo al più tardi entro 30 gg dalla ricezione della Richiesta. Altrimenti, comunica all'Interessato il motivo del ritardo, fondato su criteri oggettivi.

Nella risposta, a seconda della tipologia di Richiesta, la Segreteria fornisce le seguenti Informazioni:

Accesso:

a) le finalità del trattamento;

b) le categorie di Dati;

c) i destinatari o le categorie di destinatari a cui i Dati sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;

d) quando possibile, il periodo di conservazione dei Dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

e) l'esistenza del diritto dell'Interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei Dati o la limitazione del trattamento dei Dati che lo riguardano o di opporsi al loro trattamento;

f) il diritto di proporre reclamo a un'autorità di controllo;

g) qualora i Dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;

h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Inoltre, fornisce una copia dei Dati se richiesto dall'Interessato. La Segreteria può non fornire copia dei dati richiesti se questo può ledere i diritti e le libertà di terzi (come ad esempio nel caso di segreto industriale o proprietà intellettuale). Anche in tal caso la Segreteria fornirà riscontro all'Interessato.

Portabilità:

a) Estrazione in formato strutturato, di uso comune e leggibile da dispositivo automatico, esclusivamente dei Dati forniti dall'Interessato e creazione di un file ZIP generando una password per l'apertura di tale file.

b) Con e-mail separata: invio della password per l'accesso ai Dati (nel rispetto dei 30 giorni dalla data di ricezione della richiesta)

c) la lista dei nominativi dei soggetti ai quali eventualmente sono stati comunicati i Dati e che non sono stati nominati Responsabili del trattamento, evidenziando all'Interessato la possibilità di contattarli qualora quest'ultimo fosse interessato

Cancellazione/Rettifica/Revoca del consenso/Limitazione/Opposizione:

a) conferma dell'esecuzione di quanto richiesto

b) nominativi dei soggetti ai quali eventualmente sono stati comunicati i Dati e che non sono stati nominati Responsabili del Trattamento, evidenziando all'Interessato la possibilità di contattarli qualora quest'ultimo fosse interessato

La Segreteria salva gli eventuali documenti inviati all'Interessato (compresa tutta la corrispondenza) in un'apposita cartella e chiude il caso sul file Excel. Nel file Excel sono tracciate tutte le fasi della gestione della richiesta con i relativi dettagli, ivi inclusi i casi in cui viene data risposta negativa.

Eventuali successive modifiche operative relative alle responsabilità o alle modalità di gestione del suddetto processo relativo alle richieste degli interessati sono a cura della Presidenza/Direzione di Fondir.

6 Gli strumenti di trattamento e protezione dei Dati Personali

6.1 Il Registro delle attività di trattamento del Titolare

L'articolo 30 del GDPR prevede che ogni Titolare debba tenere un registro delle attività di Trattamento. Sono esentate dalla tenuta del Registro le imprese od organizzazioni con meno di 250 dipendenti, a meno che il trattamento effettuato:

- possa presentare un rischio per i diritti e le libertà degli Interessati;
- il trattamento non sia occasionale;
- includa il trattamento di categorie particolari di Dati Sensibili.

Il Fondo, in qualità di Titolare, ha ritenuto opportuno predisporre e mantenere il proprio Registro, consultabile presso l'ufficio del Direttore.

Eventuali successive modifiche operative relative alle responsabilità o alle modalità di gestione del suddetto Registro e del relativo processo sono a cura della Presidenza/Direzione di Fondir.

6.2 Procedura di gestione del *Data Breach*

Secondo quanto previsto dal GDPR, Fondir dovrà notificare al Garante la violazione dei Dati avvenuta, entro 72 ore dalla sua scoperta/conoscenza, senza ingiustificato ritardo, a meno che sia improbabile che tale violazione presenti un rischio per i diritti e le libertà degli Interessati.

Tale rischio si ravvisa quando il *Data Breach* potrebbe comportare l'insorgenza o l'aggravamento di danni, quali perdita del controllo dei propri Dati personali, discriminazione, furto o usurpazione di identità, perdite finanziarie, decifratura non autorizzata della pseudo-anonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei Dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo.

I *Data Breach* possono ricadere in una delle seguenti tre categorie:

- **violazione della riservatezza:** quando si verifica una non autorizzata o accidentale divulgazione o accesso ai dati personali;
- **violazione della disponibilità:** quando si verifica una perdita di accesso accidentale o non autorizzata ai dati personali o una distruzione degli stessi;
- **violazione dell'integrità:** quando si verifica una non autorizzata o accidentale alterazione dei dati personali.

Inoltre, quando la violazione è suscettibile di presentare un rischio elevato per i diritti e le libertà degli Interessati, Fondir deve altresì – salvo alcune specifiche e circoscritte eccezioni – darne comunicazione agli Interessati stessi senza ingiustificato ritardo (art.34 del GDPR).

6.2.1 Segnalazione di un *Data Breach*

Il Personale di Fondir ed i terzi nominati Responsabili del Trattamento devono riferire a Fondir ogni violazione o presunta violazione della sicurezza che possa riguardare i Dati.

La segnalazione, circostanziata e corredata di tutta l'eventuale documentazione di supporto, deve essere inviata via e-mail al Direttore di Fondir e al DPO all'indirizzo dedicato.

La segnalazione deve essere effettuata immediatamente non appena si è avuta conoscenza del fatto, ed in ogni caso, entro 3 ore dalla scoperta.

6.2.2 Analisi e valutazione delle segnalazioni

Una volta pervenuta la segnalazione, il Direttore, con supporto del DPO, dovrà effettuare un'analisi preliminare con l'obiettivo di verificare se si tratti o meno di un *Data Breach*. In caso negativo, il processo si chiude senza intraprendere ulteriori azioni.

Contrariamente, qualora si tratti di un *Data Breach*, il Direttore:

- attiva le misure tecniche già esistenti in azienda per verificare se si sia verificato un *Data Breach* contattando il Consulente IT/fornitore esterno IT;

- convoca immediatamente e comunque entro 3 ore dalla ricezione della segnalazione, i Responsabili delle altre funzioni coinvolte, affinché lo supportino nella valutazione volta ad accertare se l'episodio segnalato comporta la violazione di Dati personali;
- convoca immediatamente anche i/il Responsabili/e del trattamento, qualora la violazione riguardi un trattamento affidato a quest'ultimi/o;

Il Direttore procede ad acquisire informazioni aggiuntive sulla violazione avvenuta, e ad una valutazione complessiva del *Data Breach*, che dovrà riguardare i seguenti punti:

a) data e ora in cui si è verifica la violazione;

b) data e ora in cui si è avuta a conoscenza della violazione;

c) tipologia di dati coinvolti (Dati personali dei Dirigenti, Dati personali dei dipendenti, Dati personali di contatto, Dati personali sensibili, dati di prodotto non riconducibili a persone fisiche determinate, etc...);

d) la facilità con cui i dati oggetto di violazione possono condurre all'identificazione delle persone fisiche cui i dati si riferiscono (ad esempio, dati pseudoanonimizzati possono più difficilmente consentire l'identificazione degli interessati);

e) causa della violazione;

f) sistemi informatici/informativi coinvolti e indicazione della loro ubicazione;

g) tipologia della violazione: distruzione di dati (illecita o accidentale); perdita di dati (illecita o accidentale); modifica di dati (illecita o accidentale); divulgazione non autorizzata; accesso non consentito ai dati;

h) numero (anche approssimativo) degli interessati coinvolti;

i) conseguenze eventuali sulle persone fisiche e la gravità delle stesse;

j) l'eventuale presenza di caratteristiche particolari delle persone fisiche coinvolte (ad esempio se si tratta di persone rientranti nelle categorie protette, etc.)

k) numero di dati personali violati;

l) valutazione del rischio connesso al *Data Breach* (*elevato/non elevato*). La valutazione del livello di rischio dovrà essere connessa alla probabilità che si verifichi un danno agli interessati (es. discriminazione, furto o usurpazione d'identità, pregiudizio alla reputazione, danno economico o sociale, danni fisici, ecc..) a cui si riferiscono i "dati violati" e all'impatto della violazione (che può dipendere ad esempio, dalla tipologia di dati personali, dal numero di interessati coinvolti, dalla quantità di dati, etc.).

m) sulla base della valutazione del rischio: determinazione se si tratta di una violazione che deve essere notificata al Garante e comunicata agli Interessati.

La Segreteria, su indicazione del Direttore, procede ad una annotazione del *Data Breach* in un registro dedicato e all'archiviazione in una *directory* della documentazione raccolta, inserendo le informazioni raccolte e le valutazioni effettuate.

Il Direttore dovrà provvedere affinché vengano tempestivamente adottate le misure che consentano di minimizzare le conseguenze negative della violazione.

La Segreteria, su indicazione del Direttore, annota nel registro dedicato, l'esito della valutazione indicando, in particolare:

- se l'evento segnalato configura un *Data Breach* (oppure le ragioni dettagliate per cui l'evento non è configurabile come tale);
- le eventuali misure di contenimento adottate per interrompere o mitigare gli effetti negativi del *Data Breach*, indicate dal Consulente IT/fornitore esterno IT e/o dai Responsabili delle altre funzioni coinvolte
- la necessità di notificare il *Data Breach* al Garante (ovvero le ragioni per cui ciò non è necessario);
- nel caso non sia possibile rispettare il termine di 72 ore dalla scoperta del *Data Breach* per la notifica al Garante, le ragioni di tale ritardo;
- la necessità di comunicare il *Data Breach* agli Interessati nonché le modalità con cui provvedere (ovvero le ragioni per cui non ciò non è necessario).

6.2.3 Notificazione al Garante

Qualora, all'esito della fase di valutazione, sia emerso che il *Data Breach* debba essere notificato al Garante, vi procede il Direttore entro 72 ore dalla ricezione della segnalazione.

Se non è possibile rispettare tale termine, il Direttore provvede alla notificazione nel più breve tempo possibile, dando atto nella stessa notificazione delle ragioni del ritardo, così come già documentate nella cartella dedicata.

Eventuali successive modifiche operative relative alle responsabilità o alle modalità di gestione del suddetto processo sono a cura della Presidenza/Direzione di Fondir.

6.2.4 Comunicazione agli Interessati

Qualora all'esito della fase di valutazione sia emerso che il *Data Breach* debba essere anche comunicato agli Interessati, il Direttore vi procede nel più breve tempo possibile, tenuto conto di tutte le circostanze del caso, utilizzando le modalità individuate all'esito della fase di valutazione.

In particolare, tali comunicazioni dovranno essere effettuate per il tramite di messaggi dedicati, sui canali più opportuni, e non essere quindi inviati unitamente ad altre informazioni (quali ad esempio *newsletter*, aggiornamenti periodici o altri messaggi standard), la comunicazione deve essere intelligibile, concisa, trasparente utilizzando un linguaggio semplice e chiaro.

La comunicazione agli interessati non sarà necessaria qualora si verifichi una delle seguenti ipotesi:

- il Titolare del trattamento ha posto in essere appropriate misure tecniche ed organizzative per proteggere i dati personali prima del *Data Breach*, in particolare quelle misure idonee a rendere i dati personali incomprensibili a soggetti terzi (ad esempio in caso di pseudoanonimizzazione);
- immediatamente dopo il *Data Breach*, il Titolare del trattamento ha adottato misure idonee a scongiurare il sopraggiungere del rischio ai diritti e alle libertà degli individui (ad esempio, nel caso in cui il Titolare del trattamento abbia identificato immediatamente la persona che ha sottratto i dati, prima che questi potesse divulgarli);
- la comunicazione richiederebbe sforzi sproporzionati (in questo caso si dovrà procedere con una comunicazione pubblica o misura simile, tramite la quale gli interessati saranno informati con analoga efficacia)

Il Direttore procede come sopra, anche laddove la comunicazione agli Interessati sia imposta dal Garante, a seguito della notificazione allo stesso.

6.2.5 Analisi dettagliata

Completata la seconda fase di gestione del *Data Breach*, il Direttore dà avvio ad una dettagliata analisi finale, al fine di individuare ulteriori misure che sia opportuno/necessario adottare per evitare in futuro altri episodi analoghi di *Data Breach* ovvero, in generale, per contribuire ad una più efficace protezione dei Dati personali. Tale analisi sarà svolta dal Responsabile IT e/o dai Responsabili delle altre funzioni coinvolte.

Delle misure adottate il Consulente IT/fornitore esterno IT e/o i Responsabili delle altre funzioni coinvolte informano esaustivamente il Direttore, fornendo anche la documentazione a corredo, affinché quest'ultimo possa provvedere ad aggiornare la cartella dedicata con tali ulteriori informazioni.

Eventuali successive modifiche operative relative alle responsabilità o alle modalità di gestione del suddetto processo di *Data Breach* sono a cura della Presidenza/Direzione di Fondir.

6.3 Data Protection Impact Assessment (DPIA)

In conformità all'articolo 35 del GDPR, Fondir procede ad una DPIA in fase di progettazione di un nuovo trattamento, ad esempio in occasione dello sviluppo di ogni nuova iniziativa o servizio o di nuovi applicativi e soluzioni informatiche che possa presentare un rischio elevato per i diritti e le libertà degli Interessati.

La valutazione relativa alla presenza o meno di tale rischio deve essere effettuata di volta in volta e caso per caso, considerando le peculiarità di ciascun progetto.

In tutti i casi in cui non sia chiaro se tale rischio sia presente e quindi se sia richiesta una valutazione d'impatto sulla protezione dei dati o meno.

In generale, e salva in ogni caso la valutazione caso per caso, si può ritenere che sussista un rischio elevato in particolare qualora il trattamento presenti almeno 2 dei seguenti 9 elementi:

- profilazione, trattamenti valutativi e scoring (ad es. creazione di profili comportamentali, basati sulle scelte effettuate o sulla navigazione sul sito web): nell'ipotesi in cui trattasi di trattamenti che prevedano la valutazione o assegnazione di un punteggio, inclusiva di profilazione e previsione, in particolare in considerazione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato;
- decisioni automatizzate che producono significativi effetti giuridici o di analoga natura (ad es. inclusione o esclusione automatica, senza valutazione ulteriore, di fornitori in/da procedure di gara, sulla base dei dati forniti);
- monitoraggio sistematico (ad es. sorveglianza sistematica di aree pubbliche);
- dati "sensibili" o dati di natura estremamente personale: questo criterio include Categorie particolari di dati personali così come definite all'articolo 9 del Regolamento (ad esempio informazioni sulle opinioni politiche delle persone), nonché dati personali relativi a condanne penali o reati di cui all'articolo 10.
- trattamenti di Dati su larga scala (da determinare sulla base del numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento; volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento; durata, o persistenza, dell'attività di trattamento; ambito geografico dell'attività di trattamento);
- combinazione o raffronto di insiemi di dati (ad es. derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato);
- dati relativi a interessati vulnerabili: il trattamento di questo tipo di dati è un criterio a causa dell'aumento dello squilibrio di potere tra gli interessati e il Titolare del trattamento, aspetto che fa sì che le persone possono non essere in grado di acconsentire od opporsi al trattamento dei loro dati o di esercitare i propri diritti. Gli interessati vulnerabili possono includere i minori (i quali possono essere considerati non essere in grado di opporsi e acconsentire deliberatamente e consapevolmente al trattamento dei loro dati), i dipendenti, i segmenti più vulnerabili della popolazione che richiedono una protezione speciale (infermi di mente, richiedenti asilo o anziani, pazienti, ecc.) e, in ogni caso in cui sia possibile individuare uno squilibrio nella relazione tra la posizione dell'interessato e quella del Titolare del trattamento;
- utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative: l'uso di una nuova tecnologia può comportare la necessità di realizzare una DPIA. Ciò è dovuto al fatto che il ricorso a tale tecnologia può comportare nuove forme di raccolta e di utilizzo dei dati, magari costituendo un

rischio elevato per i diritti e le libertà delle persone. Infatti, le conseguenze personali e sociali dell'utilizzo di una nuova tecnologia potrebbero essere sconosciute.

- Trattamenti che, di per sé, "impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto". Ciò comprende i trattamenti finalizzati a consentire, modificare o negare l'accesso degli interessati a un servizio o alla stipulazione di un contratto.

La DPIA **non** è richiesta nei seguenti casi:

- quando il trattamento non è tale da "presentare un rischio elevato per i diritti e le libertà delle persone fisiche";
- quando la natura, l'ambito di applicazione, il contesto e le finalità del trattamento sono molto simili a un trattamento per il quale è stata svolta una valutazione d'impatto sulla protezione dei dati. In tali casi, si possono utilizzare i risultati della valutazione d'impatto per un trattamento analogo;
- quando le tipologie di trattamento sono state verificate da un'autorità di controllo prima del maggio 2018 in condizioni specifiche che non sono cambiate;
- qualora un trattamento sia basato su una norma di legge o un provvedimento dell'autorità garante ossia nell'eventuale elenco (stabilito dall'autorità di controllo) delle tipologie di trattamento per le quali non è richiesta alcuna valutazione d'impatto sulla protezione dei dati.

Ogni funzione interessata deve segnalare al Direttore la progettazione di un nuovo trattamento di dati personali. Il Direttore e la Funzione interessata, valutano, secondo i criteri di cui al paragrafo precedente, se lo stesso presenta o meno un rischio elevato, chiedendo anche il parere del DPO.

Se da tale valutazione emerge che il trattamento non presenta rischi, il Direttore deve giustificare e documentare all'interno del Registro delle attività di trattamento i motivi che lo hanno spinto a non effettuare una DPIA, nonché annotare il parere del DPO, a tal fine consultato.

Qualora, invece, il Direttore e la funzione interessata ritengano che il nuovo trattamento sia caratterizzato da un rischio elevato, si procede alla valutazione di impatto compilando in ogni sua parte il "Questionario DPIA".

La Funzione interessata coinvolge il DPO per un supporto e per condividere le risultanze della valutazione di impatto. Il parere del DPO, così come le decisioni prese dalla Funzione interessata nel corso dello svolgimento dell'attività, devono essere documentate all'interno della DPIA.

Qualora il trattamento venga eseguito in tutto o in parte da un Responsabile del trattamento dei dati, quest'ultimo deve assistere la Funzione interessata nella compilazione del Questionario DPIA.

Se del caso Fondir raccoglie le opinioni degli Interessati o dei loro rappresentanti sul trattamento oggetto di DPIA. L'opportunità di sentire gli interessati va valutata con il supporto del DPO.

Il Fondo può ritenere opportuno consultare esperti indipendenti che esercitano professioni diverse (avvocati, esperti informatici, esperti di sicurezza, sociologi, esperti di etica, ecc.) affinché forniscano specifico supporto nell'esecuzione della DPIA.

L'aggiornamento della valutazione d'impatto sulla protezione dei dati deve essere svolto nel corso dell'intero ciclo di vita della Tecnologia/prodotto/sistema al fine di garantire la protezione dei dati. Può essere altresì necessario ripetere singole fasi della valutazione man mano che il processo di sviluppo evolve, dato che la selezione di determinate misure tecniche od organizzative può influenzare la gravità o la probabilità dei rischi posti dal trattamento.

Eventuali successive modifiche operative relative alle responsabilità o alle modalità di gestione del suddetto processo di *DPIA* sono a cura della Presidenza/Direzione di Fondir.

7 Altri trattamenti rilevanti

7.1 Videosorveglianza

Ai sensi dell'art. 4 della L. 300/1970 (Statuto dei Lavoratori) e delle misure di tutela ivi previste, sono installate presso la sede di Fondir delle telecamere unicamente per esigenze di tutela del patrimonio del Fondo.

Il sistema di videosorveglianza risulta attualmente attivo solamente al di fuori dell'orario di lavoro, per monitorare eventuali intrusioni non autorizzate. Fondir non intende in ogni caso porre in essere un monitoraggio dell'attività dei lavoratori; tuttavia, sebbene non risulti obbligatorio, ai sensi della normativa sopra richiamata, procedere alla sottoscrizione di un accordo sindacale in riferimento all'attività di videosorveglianza, tuttavia si ritiene comunque applicabile la normativa privacy nell'eventualità in cui le immagini riprendano l'accesso di persone fisiche presso i locali di Fondir.

Pertanto, al fine di garantire il rispetto della Normativa Vigente (anche nel rispetto di specifici provvedimenti in materia) la presenza degli impianti è segnalata da una specifica informativa collocata presso la reception e da un'informativa sintetica situata nelle vicinanze di ogni telecamera.

Fondir ha provveduto, inoltre a nominare i soggetti interni che accedono alle immagini videosorvegliate quali "Autorizzati".

Il sistema di videosorveglianza risulta attualmente attivo solamente al di fuori dell'orario di lavoro, per monitorare eventuali intrusioni non autorizzate.

Eventuali successive modifiche operative relative alle responsabilità o alle modalità di gestione del suddetto processo sono a cura della Presidenza/Direzione di Fondir.

7.2 Trattamento dei dati personali tramite sistemi di Intelligenza Artificiale (AI)

Il Fondo informa che, nell'ambito della gestione delle attività formative e dei relativi processi amministrativi, potrà effettuare trattamenti di dati personali mediante sistemi di Intelligenza Artificiale ("AI"), nel rispetto del GDPR, del D.Lgs. 196/2003 come modificato, nonché dei principi di correttezza, trasparenza, minimizzazione e limitazione della finalità.

7.2.1 Finalità del trattamento tramite AI

I trattamenti svolti mediante sistemi di AI sono utilizzati esclusivamente per le seguenti finalità, strettamente connesse all'organizzazione, monitoraggio, verifica e valutazione delle iniziative formative finanziate e gestite dal Fondo:

a) verifica automatizzata dei tracciati relativi alla Formazione a Distanza (FAD), inclusi log di accesso, durata, progressi e completamento delle attività formative;

b) verifica dei registri presenza firmati dai docenti e dai discenti nelle attività in presenza;

c) controllo delle eventuali sovrapposizioni di incarichi o presenze tra docenti e/o discenti, mediante incrocio automatico dei calendari formativi e dei registri/tracciati automatici FAD;

d) analisi e valutazione della qualità didattica tramite elaborazione dei questionari di gradimento, delle relazioni finali e dei commenti testuali, anche mediante l'impiego di tecniche di Natural Language Processing (NLP).

Tali trattamenti trovano base giuridica negli artt. 6, par. 1, lett. b) ed f) GDPR, in quanto necessari per l'esecuzione di attività connesse alla gestione dei piani formativi e per il perseguimento del legittimo interesse del Fondo—adeguatamente documentato—alla verifica dell'efficacia, regolarità e qualità delle attività formative.

7.2.2 Categorie di dati trattati tramite AI

Sono trattati esclusivamente dati pertinenti e limitati alle finalità sopra indicate, tra cui:

- dati identificativi minimi (nome, cognome, ID interno, ruolo);
- tracciati FAD (log, durata, completamento moduli, eventi di connessione);
- registri presenza;
- risposte a questionari, punteggi e commenti;
- relazioni finali dei referenti aziendali.

Eventuali dati non necessari all'output sono automaticamente esclusi dal sistema AI o pseudonimizzati.

7.2.3 Modalità di funzionamento dei sistemi AI

Il trattamento tramite AI avviene attraverso processi automatizzati che effettuano:

- validazione formale dei dati raccolti;
- identificazione automatica di anomalie (es. accessi multipli, durate incoerenti, presenze sovrapposte);
- analisi testuale aggregata dei contenuti;
- generazione di indicatori, statistiche e segnalazioni ("flag") sottoposte a successiva revisione manuale.

Il Fondo assicura che i modelli adottati non conservino dati personali negli strati di addestramento e che tutte le elaborazioni siano registrate in audit log immodificabili.

7.2.4 Assenza di processi decisionali automatizzati

Il Fondo garantisce che nessun trattamento effettuato tramite AI produca effetti giuridici nei confronti dell'Interessato o incida significativamente sulla sua persona senza intervento umano ai sensi dell'art. 22 GDPR.

Ogni segnalazione prodotta dal sistema è soggetta a verifica e validazione da parte del personale autorizzato.

7.2.5 Misure di sicurezza

Il trattamento tramite AI è protetto da misure tecniche e organizzative adeguate ai sensi dell'art. 32 GDPR, tra cui:

- cifratura dei dati in transito e a riposo;
- controlli di accesso basati su ruoli;
- pseudonimizzazione ove possibile;
- logging e monitoraggio degli accessi;
- aggiornamento periodico dei modelli;
- verifica periodica del corretto funzionamento degli algoritmi;
- valutazione d'impatto (DPIA).

7.2.6 Conservazione dei dati

I dati personali trattati tramite AI sono conservati per il tempo strettamente necessario al raggiungimento delle finalità sopra indicate e nel rispetto dei tempi previsti nel Regolamento Privacy e nei documenti attuativi del Fondo.

7.2.7 Diritti degli interessati

Gli Interessati possono esercitare i diritti previsti dagli artt. 15-22 GDPR anche relativamente ai trattamenti effettuati tramite AI, con particolare riferimento a:

- diritto di ottenere l'intervento umano,
- diritto di esprimere la propria opinione,
- diritto di contestare il risultato generato dal sistema automatizzato.

8 La Governance IT

8.1 I principi del GDPR

Gli artt. da 33 a 36 del Codice Privacy, del Disciplinare Tecnico in materia di misure minime di sicurezza (Allegato B), e dell'art. 32 del GDPR, recano alcune norme per l'individuazione delle misure di sicurezza, anche minime, per il Trattamento dei Dati.

8.2 Il Codice di Condotta per l'utilizzo degli strumenti informatici del Fondo

Il Fondo ha adottato un Codice di Condotta per l'uso degli strumenti informatici con cui il Personale svolge l'attività lavorativa (*PC, TABLET, smartphone aziendali, rete internet ed intranet, posta elettronica aziendale, ...*). Il suddetto Codice di Condotta è informato al principio dall'art. 4 comma 3 della L. 300/1970 (Statuto dei Lavoratori), secondo cui le informazioni raccolte tramite gli strumenti adoperati dal lavoratore per rendere la prestazione lavorativa e quelli necessari alla registrazione degli accessi e delle presenze, possono essere utilizzate ai fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione sulle modalità d'uso degli strumenti utilizzati e di effettuazione dei controlli, nel rispetto di quanto disposto dalla Normativa Vigente.

Il Codice di Condotta per l'uso degli strumenti informatici viene consegnato al Personale al momento dell'instaurazione del rapporto contrattuale con Fondir, unitamente al welcome kit, a cura del Direttore.

Eventuali successive modifiche operative relative alle responsabilità o alle modalità di gestione del suddetto processo e del Codice di Condotta per l'uso degli strumenti informatici sono a cura della Presidenza/Direzione di Fondir.

8.3 Indirizzi sull'uso di siti e strumenti di Intelligenza Artificiale

Il Fondo ha adottato e reso vincolante per tutto il personale il documento denominato **"Indirizzi sull'Uso di Siti e Strumenti di Intelligenza Artificiale"**, che costituisce parte integrante del presente Regolamento Privacy. Tale documento disciplina l'utilizzo, da parte di dipendenti, collaboratori e soggetti operanti per conto dell'Azienda, di siti, piattaforme e strumenti basati su Intelligenza Artificiale (IA), inclusi i sistemi di IA per finalità generali (GPAI), con l'obiettivo di garantire la piena conformità alle normative vigenti in materia di protezione dei dati personali e di impiego responsabile dell'IA.

In applicazione del suddetto documento:

- è vietato l'inserimento nei sistemi di IA di dati personali, categorie particolari di dati, dati giudiziari o informazioni riservate, salvo preventiva autorizzazione del Titolare del trattamento e del DPO e previo ricorso a misure di anonimizzazione o pseudonimizzazione;
- è obbligatorio l'utilizzo esclusivo degli strumenti di IA autorizzati dall'Azienda, con particolare riferimento a Microsoft Copilot, individuato quale strumento conforme agli standard di sicurezza e protezione dei dati;
- sono definiti livelli di rischio dei sistemi di IA, conformemente all'AI Act, con divieto di impiego dei sistemi a rischio inaccettabile e restrizioni per quelli ad alto rischio;
- è previsto un obbligo di formazione specifica su uso corretto e sicuro degli strumenti di IA, nonché un obbligo di segnalazione immediata al DPO e alla Direzione in caso di anomalie, incidenti o usi non conformi.

Il mancato rispetto delle disposizioni contenute nel documento comporta l'applicazione delle misure disciplinari previste dal sistema sanzionatorio aziendale e dalla normativa vigente, ferme restando le eventuali responsabilità civili, amministrative e penali.

Il documento "Indirizzi sull'Uso di Siti e Strumenti di Intelligenza Artificiale" viene consegnato al Personale al momento dell'instaurazione del rapporto contrattuale con Fondir, unitamente al welcome kit, a cura del Direttore.
Eventuali successive modifiche operative relative alle responsabilità o alle modalità di gestione del suddetto processo e del Codice di Condotta per l'uso degli strumenti informatici sono a cura della Presidenza/Direzione di Fondir.