PIANO DI SICUREZZA

PROTEZIONE DELLE PERSONE FISICHE E TRATTAMENTO DEI DATI PERSONALI

REGOLAMENTO UE 2016/679 – GENERAL DATA PROTECTION REGULATION (GDPR)

Indice

1. FINALITÀ E DEFINIZIONI

Il presente documento viene redatto ispirandosi al Documento Programmatico per la Sicurezza (ora abrogato), il cui modello era comunque in aderenza alle disposizioni di cui al Decreto Legislativo 30 giugno 2003, n. 196, artt. da 33 a 36 (*misure minime di sicurezza*), nonchè dal disciplinare tecnico contenuto nell'allegato B del citato decreto, nonchè dal provvedimento a carattere generale del 27 novembre 2008 del Garante della Privacy.

Il documento ha la finalità di fare da riferimento per la gestione delle attività organizzative e tecniche, l'assegnazione delle responsabilità e la redazione di tutta la documentazione necessaria per conformarsi alla normativa di riferimento, anche a fini propedeutici e di ausilio all'applicazione del "REGOLAMENTO (UE) 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, che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) quale Testo rilevante ai fini del SEE (Spazio Economico Europeo).

1.1. Metodo di acquisizione e aggiornamento informazioni

La normativa italiana ed europea si applica al trattamento interamente o parzialmente automatizzato di dati. Ai fini dell'aggiornamento del presente Piano di Sicurezza, si svolge una raccolta periodica di tutte le informazioni dell'insieme delle misure tecniche e organizzative applicate sui trattamenti effettuati da tutti i soggetti interni ed esterni coinvolti, nonché del relativo monitoraggio delle misure successivamente descritte, iniziando dal seguente processo di base:

- definire le responsabilità individuando dei referenti nei vari dipartimenti;
- fornire ai dipartimenti un semplice documento dove sono descritti tutti i processi;
- prescrivere ai referenti l'obbligo di mantenere la documentazione;
- implementare un processo in ogni dipartimento per l'acquisizione delle informazioni e il loro aggiornamento;
- organizzare incontri regolari con le persone di riferimento dei dipartimenti.

Le verifiche periodiche poste in essere riguardano vari aspetti, tra i quali in breve: l'individuazione degli incaricati e le eventuali necessarie designazioni e autorizzazioni scritte, nonché i rispettivi ambiti di competenza; l'esistenza di credenziali di autenticazione e di corrette procedure di gestione, disattivazione e conservazione delle medesime; la presenza e la corretta operatività di sistemi idonei a salvaguardare la sicurezza dei servizi e l'integrità dei dati trattati quali sistemi antivirus e sistemi di firewall; le autorizzazioni agli addetti della manutenzione e gli accessi agli strumenti; la corretta gestione e conservazione dei supporti utilizzati; le procedure di accesso alle diverse aree aziendali; le necessità di formazione per rendere edotto il personale dei rischi che incombono sui dati.

Inoltre, per i trattamenti cartacei: l'accesso dati, la conservazione in archivi, la custodia degli atti e documenti, la restituzione degli atti al termine delle operazioni, la conservazione in locali muniti di serratura, l'accesso controllato agli archivi, la custodia e conservazione delle riproduzioni, ecc.

1.2. Ambiti di applicazione generali

La normativa italiana ed europea si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi.

Il regolamento Europeo si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione.

Il regolamento Europeo si applica al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano:

- l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure
- il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione.

Il regolamento Europeo si applica al trattamento dei dati personali effettuato da un titolare del trattamento che non è stabilito nell'Unione, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale.

1.3. Definizioni sui dati personali

Ai fini del regolamento europeo s'intende per «dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale; sono Categorie Speciali di Dati Personali (Art. 9 GDPR) le seguenti informazioni personali:

- Origine razziale o etnica
- Opinioni politiche
- Convinzioni religiose o filosofiche
- Appartenenza sindacale
- Vita sessuale o orientamento sessuale
- Genetici
- Biometrici
- Inerenti la salute

Nelle definizioni della normativa europea è ulteriormente specificato quanto segue:

- «dati genetici»: i 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»: i 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 relativi alla salute»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.

Ulteriori dati assimilabili alle categorie di dati speciali sono individuati nell'articolo 10 della normativa europea e riguardano il trattamento di informazioni relative a:

- condanne penali e reati

che in ambito della normativa italiana si estendeva a informazioni inerenti provvedimenti giudiziari.

1.4. Definizioni sui trattamenti

Ai fini del regolamento europeo s'intende per:

- «archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

- «trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

- «limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

- «profilazione»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

- «pseudonimizzazione»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo

di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

- «violazione dei dati personali»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

«trattamento transfrontaliero»:

- a) trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure

- b) trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;

1.5. Soggetti che trattano i dati e soggetti interessati

I soggetti che effettuano o possono effettuare trattamenti sono così definiti nel regolamento Europeo:

- «titolare del trattamento» la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

- «responsabile del trattamento» la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

- «destinatario»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

- «terzo»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

- «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;

La normativa Europea non da' una definizione di chi tratta i dati ma indica dei soggetti *autorizzati* al trattamento che nella normativa italiana sono definiti come *Incaricati* al trattamento.

Un ulteriore soggetto assimilabile alle figure autorizzate al trattamento, già individuato nella precedente legge sulla privacy era rappresentato dalla figura dell'amministratore di sistema. Tale figura è stata identificata dal Provvedimento a carattere generale del 27 novembre 2008 da parte del Garante: **Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008**

Per effetto del presente provvedimento:

- *4.1 Valutazione delle caratteristiche soggettive*

  L'attribuzione delle funzioni di amministratore di sistema deve avvenire previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza. Anche quando le funzioni di amministratore di sistema o assimilate sono attribuite solo nel quadro di una designazione quale incaricato del trattamento ai sensi dell'art. 30 del Codice, il titolare e il responsabile devono attenersi comunque a criteri di valutazione equipollenti a quelli richiesti per la designazione dei responsabili ai sensi dell'art. 29.

- 4.2 Designazioni individuali

  La designazione quale amministratore di sistema deve essere in ogni caso individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

All'interno del provvedimento sono anche individuati una serie di accorgimenti legati alla figura di *amministratore di sistema*, che saranno anch'essi presi in esame al fine di individuare eventuali misure da adottare.

1.6. Stabilimento principale

Lo «stabilimento principale» è così definito nel regolamento europeo:

> a) per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;
>
> b) con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o,

se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento.

1.7. Figure giuridiche e norme d'impresa

Le persone fisiche o giuridiche, indipendentemente dalla forma giuridica rivestita, sono così definite nel regolamento europeo :

- «rappresentante»: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;

- «impresa»: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;

- «gruppo imprenditoriale»: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;

- «norme vincolanti d'impresa»: le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune.

1.8. Autorità di controllo

Le «autorità di controllo» sono così definiti nel regolamento europeo :

- «autorità di controllo»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;

- «autorità di controllo interessata» un'autorità di controllo interessata dal trattamento di dati personali in quanto:

  a) il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo;

- b) gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure

- c) un reclamo è stato proposto a tale autorità di controllo.

1.9. Ulteriori definizioni

Sono ulteriormente definiti nel regolamento europeo :

- «obiezione pertinente e motivata»: un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione;

- «servizio della società dell'informazione»: il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio (1);

- «organizzazione internazionale»: un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.

1.10. Trasferimenti dati – Privacy Shield

Informativa - un'organizzazione deve informare le persone su:

- la sua partecipazione allo scudo per la privacy e fornire un link o l'indirizzo web per l'elenco degli scudi per la privacy;
- i tipi di dati personali raccolti e, se del caso, le entità o le filiali dell'organizzazione che aderiscono ai principi;
- il suo impegno a sottoporre ai principi tutti i dati personali ricevuti dall'UE facendo affidamento sullo scudo di privacy;
- le finalità per cui raccoglie e utilizza le informazioni personali su di loro;
- come contattare l'organizzazione per qualsiasi richiesta o reclamo, incluso qualsiasi istituto rilevante nell'UE che possa rispondere a tali richieste o reclami;
- il tipo o l'identità di soggetti terzi ai quali fornisce dati personali e le finalità per cui lo fa;
- il diritto delle persone di accedere ai propri dati personali;
- le scelte e i mezzi che l'organizzazione offre agli individui per limitare l'uso e la divulgazione dei propri dati personali;
- l'organismo indipendente di composizione delle controversie designato per trattare i reclami e fornire un ricorso appropriato gratuito all'individuo, e se sia: (1) il gruppo istituito dalle autorità di protezione dei dati, (2) un fornitore alternativo di risoluzione delle controversie con sede nell'UE o (3) un fornitore alternativo di risoluzione delle controversie con sede negli Stati Uniti;
- essendo soggetto ai poteri investigativi e esecutivi della FTC, del Dipartimento dei Trasporti o di qualsiasi altro ente giuridico autorizzato degli Stati Uniti;
- la possibilità, a determinate condizioni, per l'individuo di invocare un arbitrato vincolante;
- l'obbligo di divulgare informazioni personali in risposta a richieste lecite da parte delle autorità pubbliche, anche per soddisfare i requisiti di sicurezza nazionale o di applicazione della legge, e
- la sua responsabilità in caso di trasferimenti successivi a terzi.

Scelta - l’organizzazione deve:

- offrire agli individui l'opportunità di scegliere (optare per l'esclusione) se le loro informazioni personali sono (I) divulgabili a terzi o (II) da utilizzare per uno scopo materialmente diverso dallo scopo/i per cui è stato originariamente raccolto o successivamente autorizzato dagli individui. Gli individui devono essere dotati di meccanismi chiari, ben visibili e prontamente disponibili per esercitare la scelta;

- in deroga al punto precedente, non è necessario fornire una scelta quando la divulgazione è fatta a una terza parte che agisce come un agente per eseguire attività per conto e sotto le istruzioni dell'organizzazione. Tuttavia, un'organizzazione deve sempre stipulare un contratto con l'agente.

- Per informazioni sensibili (ad es. Informazioni personali che specificano condizioni mediche o sanitarie, origine razziale o etnica, opinioni politiche, convinzioni religiose o filosofiche, appartenenza sindacale o informazioni che specificano la vita sessuale dell'individuo), le organizzazioni devono ottenere consenso espresso affermativo (*opt in*) da individui se tali informazioni devono essere (I) divulgate a terzi o (II) utilizzate per uno scopo diverso da quelli per i quali sono state originariamente raccolte o successivamente autorizzate dai singoli attraverso l'esercizio della scelta di opt-in. Inoltre, un'organizzazione dovrebbe considerare come sensibili tutte le informazioni personali ricevute da una terza parte laddove la terza parte lo identifichi e lo consideri come sensibile.

2. ORGANIZZAZIONE E PROFILI DI AUTORIZZAZIONE

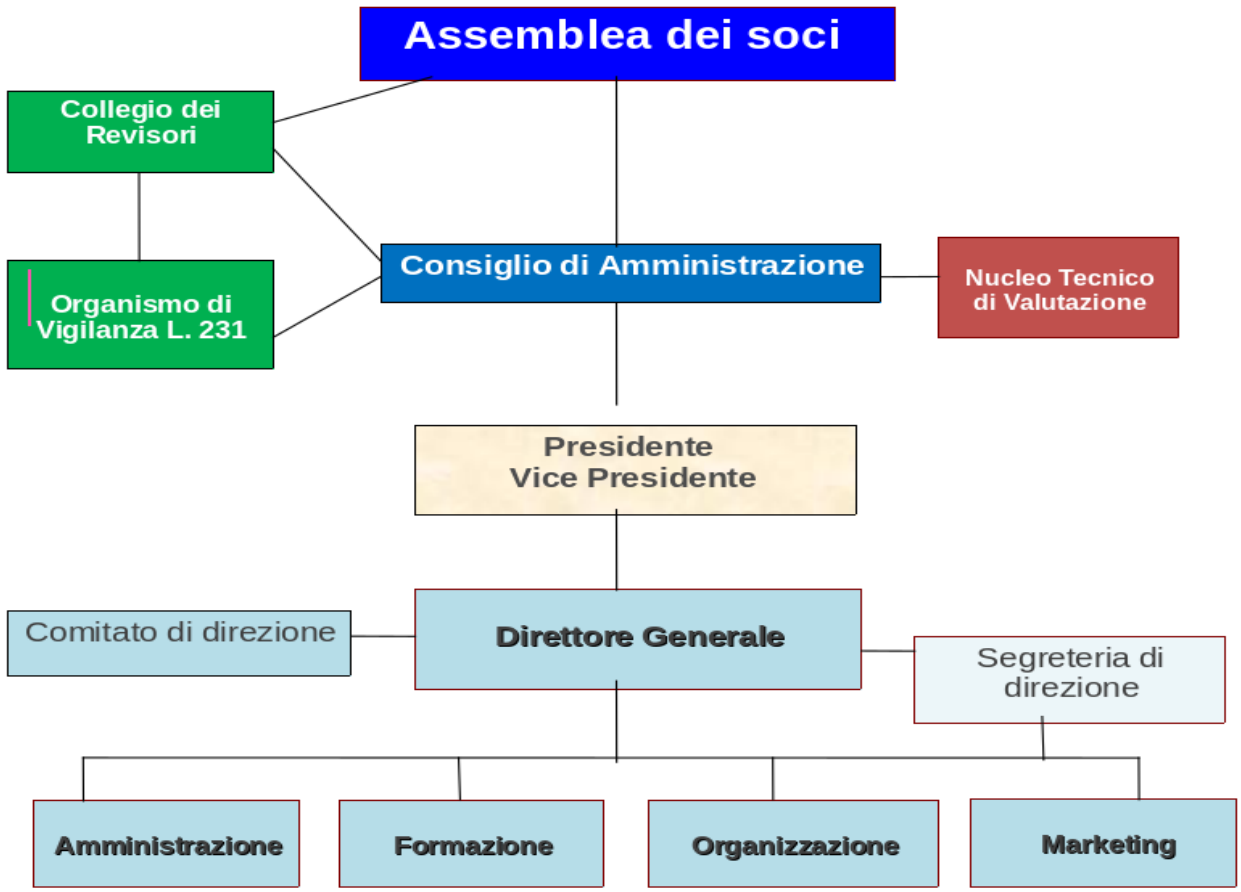
In questo capitolo è descritta l'organizzazione aziendale con le inerenti responsabilità e profili di utenza, in relazione ai processi di trattamento effettuati a seguito delle attività operative svolte.

Fapi - Fondo Formazione PMI – è un Fondo interprofessionale paritetico costituito da CONFAPI, CGIL, CISL e UIL al fine di promuovere lo sviluppo della formazione continua nelle PMI, quale strumento di competitività delle imprese e di garanzia occupazionale per i lavoratori.

Il Fondo non ha fini di lucro: promuove e finanzia piani formativi aziendali, territoriali, settoriali, regionali, interregionali e nazionali di e tra imprese concordati tra le parti, in coerenza con la programmazione regionale e con le funzioni di indirizzo attribuite in materia al Ministero del Lavoro e delle Politiche Sociali.

Il Fapi, come tutti i fondi interprofessionali, raccoglie lo 0,30% dei contributi che le imprese versano all'INPS ogni mese e che dall'INPS vengono versate ai fondi cui le aziende aderiscono. Tali risorse sono utilizzate dal Fapi per finanziarie le attività formative dei lavoratori e delle lavoratrici delle imprese aderenti.

Diagramma organizzazione



La Corporate Governance di Fapi è definita all'interno dello Statuto del Fondo. Di seguito si riportano gli organi di governo e controllo istituiti:

Assemblea: l'assemblea è composta in maniera paritetica da 12 membri di cui 6 nominati dalla CONFAPI e 6 nominati da CGIL, CISL e UIL. I membri dell'assemblea durano in carica 3 anni e possono essere rinominati. L'assemblea nomina il Presidente del Fondo su designazione della CONFAPI e il Vice Presidente su designazione di CGIL, CISL e UIL. Il Presidente e il Vice Presidente del Fondo sono anche, rispettivamente, Presidente e Vice Presidente dell'Assemblea e del Consiglio di Amministrazione. I poteri dell'Assemblea sono disciplinati dall'art. 8 dello Statuto.

Presidente e Vice Presidente: al Presidente spetta rappresentare il Fondo di fronte a terzi e stare in giudizio; il Vice Presidente coadiuva il Presidente nello svolgimento delle sue funzioni. I poteri di Presidente e Vicepresidente sono disciplinati dall'art. 9 dello Statuto.

Consiglio di Amministrazione: l'amministrazione di Fapi è affidata ad un consiglio di amministrazione composto in maniera paritetica da 6 membri, di cui il Presidente e 2 membri designati dalla CONFAPI e il Vice Presidente e 2 membri designati da CGIL, CISL e UIL. I consiglieri di amministrazione durano in carica tre anni e sono rieleggibili. Al Consiglio di Amministrazione spettano i poteri di ordinaria e straordinaria amministrazione del Fondo, disciplinati in dettaglio dall'art. 10 dello Statuto.

Collegio dei Revisori dei conti: il collegio dei Revisori di Fapi è composto da 3 membri effettivi. Questi sono così designati: uno dalla CONFAPI, uno congiuntamente da CGIL, CISL e UIL, il terzo con funzioni di Presidente, nominato dal Ministero del Lavoro e delle Politiche Sociali. CGIL, CISL e UIL designano inoltre 2 membri supplenti destinati a sostituire i membri effettivi (eventualmente assenti). I revisori (sia effettivi che supplenti) durano in carica 3 anni e possono essere rinominati. Il Presidente del Collegio dei Revisori deve essere iscritto all'Albo dei Revisori dei Conti.

La struttura organizzativa di Fapi, ispirata al principio della separazione di compiti, ruoli e responsabilità tra le funzioni operative e quelle di controllo, è articolata come descritto nell'apposito organigramma.

- L'organigramma di Fapi individua le seguenti figure/aree:
- Presidente e Vice Presidente del Fondo;
- Direttore Generale del Fondo;
- Comitato di Direzione, composto dal Direttore Generale e dai quattro responsabili delle Aree operative e cioè: Amministrazione, Formazione, Organizzazione e Marketing.
- Uffici Amministrazione, Formazione, Organizzazione, Marketing, Segreteria

Le strutture organizzative che operano trattamenti di dati personali con propri processi di riferimento, per i quali si definiranno i profili di utenza di accesso ai dati personali possono essere rappresentati come segue:

- Direzione Generale e Segreteria;
- Amministrazione;
- Formazione;
- Organizzazione;
- Marketing.

Sono anche presenti dei profili di utenza adibiti alla lettura e gestione di dati in relazione a processi di trattamento derivati delle strutture precedentemente descritte, che sono:

- Consiglio di Amministrazione;
- Collegio dei Revisori
- Nucleo Tecnico di valutazione.

2.1. Direzione Generale e Segreteria

Il **Direttore Generale** dirige e coordina l'attività degli Uffici, in rapporto diretto con i Responsabili delle aree operative e nell'ambito del Comitato di Direzione.

Riferisce alla Presidenza, al Consiglio di Amministrazione, al Collegio dei Sindaci Revisori dei Conti, all'Assemblea dei Soci, partecipando alle riunioni degli organi statutari in qualità di segretario, preparando i materiali per lo svolgimento dei lavori e curando la verbalizzazione delle sedute e la stesura delle deliberazioni.

Coordina i lavori dei Comitati e Gruppi di lavoro costituiti del Fondo.

Esercita i poteri di firma nelle forme e nei termini stabiliti dallo statuto e dalle deliberazioni del CDA.

Predispone, in collaborazione con l'Ufficio Amministrazione e sentiti gli altri Uffici, la documentazione necessaria per la stesura dei bilanci consuntivo e previsionale del Fondo e presenta i bilanci al Consiglio di Amministrazione.

Predispone periodici rapporti sull'attività del Fondo, da presentare al Consiglio di Amministrazione.

Supporta il coordinamento delle attività sul territorio limitatamente agli aspetti politico-strategici connessi alla presenza delle parti socie sul territorio e alle tematiche della bilateralità.

E' responsabile, a supporto della Presidenza, dei rapporti istituzionali a qualsiasi livello intrattenuti dal Fondo, in particolare con:

- Il Ministero del Lavoro e delle Politiche Sociali
- L'ANPAL
- Altri Ministeri e Uffici governativi competenti in materia di formazione e lavoro
- L'INPS
- L'INAIL
- Gli altri Fondi Interprofessionali Nazionali per la Formazione Continua
- Le Associazioni di categoria e i Sindacati dei lavoratori
- Gli assessorati regionali alla Formazione e Lavoro

Cura i rapporti con la stampa, con il supporto dell'Ufficio Marketing, e mantiene i rapporti con i consulenti legali del Fondo.

Coordina il Comitato di Direzione, composto dai responsabili delle quattro aree, che svolge i compiti di cui alla delibera CdA n. 40 del 25 settembre 2008.

La **Segreteria di Direzione** svolge le seguenti funzioni e compiti:

- preparazione, cura, conservazione e archiviazione della documentazione (convocazioni, archiviazione dei verbali, conservazione dei documenti prodotti) del Consiglio di Amministrazione, dell'Assemblea dei Soci, del Collegio dei Sindaci Revisori dei Conti, dell'Organismo di Vigilanza L. 231 e del Comitato di Direzione;
- preparazione, cura, conservazione e archiviazione della documentazione

(convocazioni, archiviazione dei verbali, conservazione dei documenti prodotti) di tutti i Comitati, le Commissioni, le Consulte e i Gruppi di lavoro, anche costituiti ad hoc e in via temporanea, quali le Commissioni giudicatrici di gara e simili;
- gestione del workflow delle cartelline di lavoro del CdA e dell'Assemblea, e di tutte le pratiche connesse;
- tenuta e vidimazione dei libri verbali del Consiglio di Amministrazione e dell'Assemblea dei Soci;
- archiviazione e conservazione degli atti riguardanti le gare d'appalto e le procedure ristrette di licitazione per l'affidamento di servizi o l'acquisizione di beni da soggetti esterni;
- protocollo della corrispondenza cartacea, elettronica e fax in entrata e in uscita;
- centralino telefonico;
- fattorinaggio esterno ed interno;
- assistenza alla Direzione, alla Presidenza, al Collegio dei Sindaci Revisori dei Conti e all'Organismo di Vigilanza ex L. 231;
- tenuta dei rapporti con i fornitori anche per la manutenzione dei macchinari e verifica delle scorte di cancelleria e dei materiali di consumo;
- assistenza tecnica di primo livello agli attuatori dei Piani formativi finanziati, a supporto dell'Ufficio Formazione;
- gestione del servizio di helpdesk di primo livello verso i soggetti presentatori di Piani formativi a supporto dell'Ufficio Marketing.

<u>Personale addetto e profili di accesso:</u>

- 1 direttore Giorgio Tamaro Profilo DSR
- 1 addetto Francesca Nati Profilo DS1
- 1 addetto Raffaella Priaro Profilo DS1

2.2. Amministrazione

L'Ufficio Amministrazione ha le seguenti funzioni e compiti:

- tenuta della contabilità;
- cassa e banche;
- rilevazione delle entrate;
- pagamenti relativi alla gestione dell'ente;
- pagamenti di acconti e saldi delle attività formative finanziate;
- predisposizione in bozza dei documenti di bilancio preventivo;
- predisposizione in bozza e con l'ausilio del consulente incaricato dei documenti di bilancio consuntivo;
- predisposizione periodica di reportistica di cassa;
- monitoraggio finanziario semestrale da trasmettere al Ministero del Lavoro e/o all'ANPAL in ottemperanza alla normativa vigente;
- stesura, cura e conservazione dei contratti disciplinanti i rapporti con fornitori di beni e servizi a qualsiasi titolo;
- gestione delle istruttorie di finanziamento dei Piani e Progetti formativi (controllo delle fideiussioni, gestione degli acconti e dei saldi, richieste di proroghe delle fidejussioni in scadenza per i Piani non integralmente conclusi dal punto di vista amministrativo e svincoli delle stesse in caso di piani con iter amministrativo completo);
- assistenza tecnica agli attuatori dei piani formativi in relazione alle richieste di chiarimenti e di informazioni sulle modalità di richiesta di acconti e saldi e sulle fidejussioni;
- assistenza tecnica agli operatori delle Articolazioni Regionali sulle pratiche amministrative;
- cura e conservazione delle pratiche di liquidazione di saldi ed acconti;
- amministrazione del personale e gestione dei rapporti con il consulente del lavoro per gli adempimenti relativi;
- ufficio acquisti e approvvigionamenti.

<u>Personale addetto e profili di accesso:</u>

- 1 responsabile Daniela Pengue Profilo AR
- 1 addetto Fabio Piccirilli Profilo A1
- 1 addetto Caterina Toscano Profilo A1

2.3. Formazione

L'Ufficio Formazione ha le seguenti funzioni e compiti:

- redazione dell'Offerta formativa annuale;
- predisposizione degli Avvisi e degli eventuali altri dispositivi per il finanziamento della formazione;
- definizione delle procedure di finanziamento della formazione di propria competenza, anche informatizzate.
- stesura ed aggiornamento del Manuale di Gestione sulla base delle indicazioni degli Uffici competenti ed esaminati in Comitato di Direzione;
- stesura ed aggiornamento del Regolamento per le aree di propria competenza;
- espletamento delle procedure inerenti la gestione delle attività formative, preparazione, stipula delle convenzioni, allestimento e conservazione dei fascicoli dei Piani, della corrispondenza relativa ecc.;
- gestione delle proroghe, variazioni e deroghe su tempistica, partecipanti ed aziende in norma e fuori norma, anche da sottoporre al CdA;
- gestione procedure di rinuncia Piani e Progetti in itinere e di revoca Piani per non attuazione dell'attività finanziata;
- raccordo con l'Ufficio Marketing per l'organizzazione dell'help desk per i soggetti proponenti nella fase di presentazione dei Piani formativi (*help desk presentazione Piani*);
- raccordo con il Nucleo Tecnico di Valutazione Nazionale e la Direzione per la predisposizione, l'avvio e la conclusione del procedimento di valutazione dei Piani formativi presentati, nonché per la predisposizione documentale relativa alle graduatorie da sottoporre al CdA;
- raccordo con il Nucleo Tecnico di Valutazione Nazionale e la Direzione per la presa in carico delle richieste di riesame verificate dal Comitato dei Garanti da sottoporre al CdA;
- raccordo con l'Ufficio Organizzazione e la Direzione per gli adempimenti richiesti per la verifica RNA;
- assistenza tecnica agli attuatori dei piani formativi sulle pratiche inerenti la gestione delle attività formative dei Piani finanziati (*help desk gestione Piani*)
- supervisione della reportistica, del rapporto Fapi sulle attività formative finanziate e dei quaderni del Fapi.

<u>Personale addetto e profili di accesso:</u>

- 1 responsabile Tania Grandi Profilo FR
- 1 addetto Silvia Cautillo Profilo F1
- 1 addetto Valeria Volpe Profilo F1

2.4. Organizzazione

L'Ufficio Organizzazione ha le seguenti funzioni e compiti:

- gestione dei rapporti con le Articolazioni Regionali per la parte riguardante le attività di funzionamento;
- gestione delle procedure di monitoraggio fisico semestrale nei confronti del Ministero del Lavoro;
- supervisione delle procedure di controllo in itinere e finale dei Piani e Progetti finanziati svolte dalla Società esterna fornitrice del servizio;
- gestione delle pratiche relative ai controlli in itinere e finali (verbali di ispezione) e trasmissione all'Ufficio Amministrazione delle pratiche stesse per la liquidazione dei contributi;
- gestione delle variazioni di calendario in norma e fuori norma;
- gestione delle procedure di rinunce, riparametrazioni e revoche dei Piani e Progetti finanziati;
- controllo dei rendiconti finali di spesa relativi alle attività delle Articolazioni Regionali e trasmissione all'Ufficio Amministrazione delle pratiche stesse per la liquidazione dei contributi;
- controllo dei rendiconti finali di spesa dei soggetti attuatori delle attività propedeutiche e trasmissione all'Ufficio Amministrazione delle pratiche stesse per la liquidazione dei contributi;
- supervisione della piattaforma informatica sviluppata e gestita dalla Società esterna fornitrice del servizio e rapporti con la Società stessa;
- referente per il funzionamento delle attrezzature informatiche (hardware e software) del Fondo;
- gestione delle pratiche relative al comparto sicurezza e salute della struttura interna del Fondo e rapporti con i consulenti esterni del servizio.

<u>Personale addetto e profili di accesso:</u>

- 1 responsabile Maria Rita Evangelista Profilo OR
- 1 addetto Roberto Ciavarro Profilo O1
- 1 addetto Claudio Cortina Profilo O1
- 1 addetto Francesco Faggella Profilo O1

2.5. Marketing, promozione e comunicazione, helpdesk

L'Ufficio Marketing ha le seguenti funzioni e compiti:

- attività di marketing, promozione, pubblicità e sviluppo del Fondo;
- gestione dei rapporti con il territorio per la parte riguardante le attività di marketing, promozione e sviluppo;
- cura e supervisione del portale Fapi e della newsletter, incluso l'inserimento e l'aggiornamento delle informazioni sul sito del Fondo;
- organizzazione di convegni, manifestazioni e rapporti con la stampa;
- gestione dei rapporti con l'INPS, soprattutto riguardo il data base delle iscrizioni, cancellazioni e controllo dei records degli iscritti;
- gestione, monitoraggio e aggiornamento dei dati riguardanti le adesioni al Fondo, inclusi i rapporti con i soggetti (aziende e lavoratori) interessati;
- predisposizione dei rapporti periodici sullo stato delle adesioni al Fondo;
- gestione delle pratiche relative alla mobilità e alla portabilità da e verso altri Fondi;
- predisposizione e gestione degli atti riguardanti le gare d'appalto e le procedure ristrette di licitazione per l'affidamento di servizi o l'acquisizione di beni da soggetti esterni e trasmissione alla segreteria di tutti gli atti per la conservazione degli stessi;
- gestione del servizio di helpdesk di primo livello verso i soggetti presentatori di Piani e progetti formativi.

Personale addetto e profili di accesso:

• 1 responsabile	*attualmente ricoperto dal direttore*	Profilo MR
• 1 addetto	Claudio De Francesco	Profilo M1
• 1 addetto	Fabrizio Faraco	Profilo M1

3. REGISTRO DEI TRATTAMENTI

Il FAPI a seguito delle funzioni di competenza sopra descritte tratta i seguenti dati personali comuni:

- dati personali non sensibili dei clienti, dei fornitori o di terzi ricavati o ricavabili da elenchi pubblici, albi professionali o camerali;

- dati personali non sensibili dei clienti, forniti dagli stessi per l'espletamento delle attività aziendali del titolare del trattamento;

- dati personali non sensibili dei dipendenti e dei collaboratori, necessari al regolare svolgimento del rapporto di lavoro o di collaborazione, nonché quelli affidati al datore di lavoro per esigenze di natura bancaria.

Il FAPI tratta i seguenti dati particolari sensibili:

- dati sensibili del personale dipendente, idonei a rivelare lo stato di salute e le indicazioni sindacali

Il FAPI tratta i seguenti dati particolari inerenti procedimenti giudiziari:

- dati giudiziari dei dipendenti in relazione ad eventuali procedimenti giudiziari;
- dati giudiziari dei clienti in relazione ad eventuali procedimenti giudiziari per contenziosi sulle modalità e congruità della rendicontazione;
- dati giudiziari di fornitori e clienti in relazione a casellario giudiziario/carichi pendenti.

Nelle tabelle che seguono si elenca schematicamente un registro di riferimento delle attività di trattamento, in relazione ai trattamenti effettuati, direttamente o attraverso collaborazioni esterne esistenti alla data di redazione, con ogni utile informazione in conformità alla normativa italiana e all'articolo 30 del GDPR.

La sede centrale del FAPI dove attualmente sono localizzate una parte delle banche dati ove sono effettuati i trattamenti su dati personali è la seguente:

- FAPI, Sede centrale operativa Piazza del Gesù, 46 – 00186 Roma

Presso tale sede sono presenti una parte dei dati su supporto informatico e tutti i dati presenti su supporto cartaceo, questi ultimi sono distribuiti tra gli uffici del secondo piano e il magazzino del piano seminterrato.

Ulteriori banche di dati personali sono presenti esternamente alla sede del FAPI, presso la sede del Data Center del fornitore di servizi informatici Unidata:

- UNIDATA, Sede Data Center, Commercity, Viale A. G. Eiffel 100, 00148 - Roma

Presso tale sede sono presenti le banche di dati personali su supporto elettronico dei piani formativi, I dati risiedono all'interno dei server e storage di proprietà del FAPI ove UNIDATA offre servizi di housing per la componente di facility e network connectivity, e di hosting per i servizi di backup.

Ulteriori banche di dati personali possono essere trattati su supporti cartacei e informatizzati da soggetti esterni al FAPI, anche localizzati esternamente, per conto delle

società proprietarie dei software contrattualizzati in licenza di uso e per società di auditing dei piani formativi e di consulenza aziendale, fiscale e legale.

Le tabelle relative al censimento dei processi/macro attività delle banche dati, saranno suddivise inizialmente se operate come soggetti titolari e responsabili (in caso di trattamenti di dati operati per conto di eventuali clienti), e poi saranno successivamente classificate per unità principale di struttura organizzativa di riferimento.

Censimento delle attività di trattamento Ai sensi dell'articolo 30(1) Titolare GDPR	
Estremi identificativi del Titolare Nome e informazioni di contatto della persona fisica / giuridica / agenzia / organismo ecc. Nome : Dott. Francesco Lippi Indirizzo: via Ing. Antonio Argiolas 40 CAP – Città: Cagliari Telefono : 342 8930 655 Indirizzo E-Mail: presidente@fondopmi.it Internet URL: www.fondopmi.com	
Estremi identificativi del Rappresentante del Titolare Nome e informazioni di contatto della persona fisica / giuridica / agenzia / organismo ecc. Nome : Dott. Giorgio Tamaro indirizzo: vicolo della Serpe 75 CAP - Città : 00149 Roma Telefono : 380 3180 294 Indirizzo E-Mail: direzione@fondopmi.it Internet URL: www.fondopmi.com	
Estremi identificativi del Responsabile della Protezione dei Dati * (se esterno, fornire indirizzo) * nella misura in cui un DPO è stato nominato ai sensi dell'Articolo 37 GDPR Dati personali Cognome, Nome indirizzo CAP - Città Telefono Indirizzo E-Mail	

3.1. Direzione Generale e Segreteria

Di seguito sono descritti i processi con le informazioni e le modalità con cui i trattamenti sono operati:

Attività di Trattamento: **Identificativo: Protocollazione e comunicazioni**	**indice N. 1:**
Data di inizio:	Data della modifica più recente:

Struttura organizzativa Punto di Contatto Telefono Indirizzo E-Mail (Art. 30(1)(2)(a) GDPR)	Direzione Generale e Segreteria Dott. Giorgio Tamaro
Finalità del trattamento (Art. 30(1)(2)(b) GDPR)	Gestione delle attività di protocollazione della documentazione in entrata e in uscita, sia quella privata della Direzione Generale che di quella generale in relazione a tutte le altre strutture dell'organizzazione. Gestione delle comunicazioni in uscita e del relativo archivio storico.
Descrizione delle Categorie delle materie dei dati interessati (Art. 30(1)(2)(c) GDPR)	☒ Dipendenti ☐ Candidati ☒ Fornitori ☒ Soggetti attuatori ☐ Tirocinanti ☒ Consulenti ☒ Collaboratori ☒ Destinatari finali
Descrizione delle Categorie dei Dati Personali (Art. 30(1)(2)(c) GDPR)	☒ Personali identificativi ☐ ☐ Categorie Speciali di Dati Personali (Art. 9 e Art. 10 GDPR): ☐ Origine razziale o etnica ☐ Opinioni politiche ☐ Convinzioni religiose o filosofiche ☐ Appartenenza sindacale ☐ Vita sessuale o orientamento sessuale ☐ Genetici ☐ Biometrici ☐ Inerenti alla salute ☒ Provvedimenti giudiziari

Base Giuridica (Art 6 a/b/c/d/f)	a b c d e f ☐ ☒ ☐ ☐ ☐ ☐
	Informativa e modalità raccolta consenso Contratti
Categorie di Destinatari a cui i dati personali sono stati o saranno comunicati (Art. 30(1)(2)(d) GDPR)	Destinatari interni (Altre strutture che concorrono al trattamento) ☐ Direzione Generale e Segreteria ☒ Amministrazione ☒ Formazione ☒ Organizzazione ☒ Marketing ☒ Consiglio di Amministrazione ☐
	Destinatari Esterni (Categorie di Destinatari) ☐ Consulenti Fiscali, finanziari, legali e del lavoro ☐ Banche ☐ Istituti di assicurazione e previdenza ☐ Uffici delle imposte ☒ Collegio dei Revisori dei conti ☐ ☐ ☐
	Paesi terzi o Organizzazioni internazionali (Categorie) ☐ ☐ ☐ ☐

Se applicabile, Trasferimento di Dati Personali verso Paesi Terzi o Organizzazioni internazionali (Art. 30(1)(2)(e) GDPR) Identificazione dei Destinatari dei trasferimenti specifici	☒ Non si effettuano Trasferimenti e non sono previsti ☐ Trasferimenti che vengono effettuati sono i seguenti: ☐ Paesi terzi o Organizzazioni internazionali (identificare mediante nome)
A condizione che i Trasferimenti siano sottoposti alle disposizione dell' Art. 49(1) para. 2 GDPR [*Nota: Questi sono trasferimenti una tantum interessati da un "numero limitato" di individui considerati in base a "interessi legittimi impellenti"]:*	Documentazione delle garanzie sufficienti per i Trasferimenti
Conservazione/Eliminaz. e Tempi per le Varie Categorie di Dati Personali (Art. 30(1)(2)(f) GDPR)	☐ Termini di legge o sino a revoca o diritto di opposizione ☐ Da contratto ☒ Termini di conservazione amministrativi
Sistemi IT e Applicativi	☒ Office automation su repository locali ☐ Office automation su cartelle in servizi in cloud ☒ Altre applicazioni (protocollo) In previsione adozione della Information Workers Group application
Localizzazione dei dati e dei supporti di backup	☒ Cartaceo In corridoio presso sede in Piazza del Gesù e nell'archivio storico nei sotterranei ☒ Office automation su cartelle di file server Stanza Server presso sede in Piazza del Gesù, backup in loco ☒ Altre applicazioni Information Workers Group application presso Stanza Server in sede operativa in Piazza del Gesù, backup in loco

Attività di Trattamento: **Identificativo: Procedure di affidamento**	**indice N. 2:**
Data di inizio:	Data della modifica più recente:

Struttura organizzativa Punto di Contatto Telefono Indirizzo E-Mail (Art. 30(1)(2)(a) GDPR)	Direzione Generale e Segreteria Dott. Giorgio Tamaro
Finalità del trattamento (Art. 30(1)(2)(b) GDPR)	Predisposizione e gestione degli atti riguardanti le gare d'appalto e le procedure ristrette di licitazione per l'affidamento di servizi o l'acquisizione di beni da soggetti esterni e trasmissione alla segreteria di tutti gli atti per la conservazione degli stessi. I fornitori sono attinti per le gare sotto soglia attraverso un albo denominato elenco fornitori.
Descrizione delle Categorie delle materie dei dati interessati (Art. 30(1)(2)(c) GDPR)	☐ Dipendenti ☐ Candidati ☒ Fornitori ☐ Soggetti attuatori ☐ Tirocinanti ☒ Consulenti ☒ Collaboratori ☐ Destinatari finali

Descrizione delle Categorie dei Dati Personali (Art. 30(1)(2)(c) GDPR)	☒ Personali identificativi ☐ ☐ Categorie Speciali di Dati Personali (Art. 9 e Art. 10 GDPR): ☐ Origine razziale o etnica ☐ Opinioni politiche ☐ Convinzioni religiose o filosofiche ☐ Appartenenza sindacale ☐ Vita sessuale o orientamento sessuale ☐ Genetici ☐ Biometrici ☐ Inerenti alla salute ☒ Provvedimenti giudiziari
Base Giuridica (Art 6 a/b/c/d/f)	a b c d e f ☐ ☒ ☐ ☐ ☐ ☐
	Informativa e modalità raccolta consenso Contratto

Categorie di Destinatari a cui i dati personali sono stati o saranno comunicati (Art. 30(1)(2)(d) GDPR)	Destinatari interni (Altre strutture che concorrono al trattamento) ☐ Direzione Generale e Segreteria ☒ Amministrazione ☒ Formazione ☒ Organizzazione ☒ Marketing ☒ Consiglio di Amministrazione ☐
	Destinatari Esterni (Categorie di Destinatari) ☐ Consulenti Fiscali, finanziari, legali e del lavoro ☐ Banche ☐ Istituti di assicurazione e previdenza ☐ Uffici delle imposte ☒ Componenti esterni delle commissioni giudicatrici ☒ Collegio dei Revisori dei conti ☐ ☐
	Paesi terzi o Organizzazioni internazionali (Categorie) ☐ ☐ ☐ ☐

Se applicabile, Trasferimento di Dati Personali verso Paesi Terzi o Organizzazioni internazionali (Art. 30(1)(2)(e) GDPR) Identificazione dei Destinatari dei trasferimenti specifici	☒ Non si effettuano Trasferimenti e non sono previsti ☐ Trasferimenti che vengono effettuati sono i seguenti: ☐ Paesi terzi o Organizzazioni internazionali (identificare mediante nome)
A condizione che i Trasferimenti siano sottoposti alle disposizione dell' Art. 49(1) para. 2 GDPR [*Nota: Questi sono trasferimenti una tantum interessati da un "numero limitato" di individui considerati in base a "interessi legittimi impellenti"]:*	Documentazione delle garanzie sufficienti per i Trasferimenti
Conservazione/Eliminaz. e Tempi per le Varie Categorie di Dati Personali (Art. 30(1)(2)(f) GDPR)	☐ Termini di legge o sino a revoca o diritto di opposizione ☐ Da contratto ☒ Termini di conservazione amministrativi
Sistemi IT e Applicativi	☒ Office automation su repository locali ☐ Office automation su cartelle in servizi in cloud ☐ Altre applicazioni
Localizzazione dei dati e dei supporti di backup	☒ Cartaceo In stanza Direzione presso sede in Piazza del Gesù e nell'archivio storico nei sotterranei ☒ Office automation su cartelle di file server Stanza Server presso sede in Piazza del Gesù, backup in loco ☐ Altre applicazioni

Attività di Trattamento: **Identificativo: Procedure legali**	**indice N. 3:**
Data di inizio:	Data della modifica più recente:

Struttura organizzativa Punto di Contatto Telefono Indirizzo E-Mail (Art. 30(1)(2)(a) GDPR)	Direzione Generale e Segreteria Dott. Giorgio Tamaro
Finalità del trattamento (Art. 30(1)(2)(b) GDPR)	Attività di gestione dei rapporti con i legali del fondo
Descrizione delle Categorie delle materie dei dati interessati (Art. 30(1)(2)(c) GDPR)	☒ Dipendenti ☐ Candidati ☒ Fornitori ☒ Soggetti attuatori ☐ Tirocinanti ☒ Consulenti ☒ Collaboratori ☐ Destinatari finali
Descrizione delle Categorie dei Dati Personali (Art. 30(1)(2)(c) GDPR)	☒ Personali identificativi ☐ ☐ Categorie Speciali di Dati Personali (Art. 9 e Art. 10 GDPR): ☐ Origine razziale o etnica ☐ Opinioni politiche ☐ Convinzioni religiose o filosofiche ☐ Appartenenza sindacale ☐ Vita sessuale o orientamento sessuale ☐ Genetici ☐ Biometrici ☐ Inerenti alla salute ☒ Provvedimenti giudiziari

Base Giuridica (Art 6 a/b/c/d/f)	a b c d e f ☐ ☒ ☐ ☐ ☐ ☐
	Informativa e modalità raccolta consenso
Categorie di Destinatari a cui i dati personali sono stati o saranno comunicati (Art. 30(1)(2)(d) GDPR)	Destinatari interni (Altre strutture che concorrono al trattamento) ☐ Direzione Generale e Segreteria ☒ Amministrazione ☒ Formazione ☒ Organizzazione ☐ Marketing ☒ Consiglio di Amministrazione ☐
	Destinatari Esterni (Categorie di Destinatari) ☒ Consulenti Fiscali, finanziari, legali e del lavoro ☐ Banche ☐ Istituti di assicurazione e previdenza ☐ Uffici delle imposte ☒ Collegio dei Revisori dei conti ☐ ☐ ☐
	Paesi terzi o Organizzazioni internazionali (Categorie) ☐ ☐ ☐ ☐

Se applicabile, Trasferimento di Dati Personali verso Paesi Terzi o Organizzazioni internazionali (Art. 30(1)(2)(e) GDPR) Identificazione dei Destinatari dei trasferimenti specifici	☒ Non si effettuano Trasferimenti e non sono previsti ☐ Trasferimenti che vengono effettuati sono i seguenti: ☐ Paesi terzi o Organizzazioni internazionali (identificare mediante nome)
A condizione che i Trasferimenti siano sottoposti alle disposizione dell' Art. 49(1) para. 2 GDPR [*Nota: Questi sono trasferimenti una tantum interessati da un "numero limitato" di individui considerati in base a "interessi legittimi impellenti"]:*	Documentazione delle garanzie sufficienti per i Trasferimenti
Conservazione/Eliminaz. e Tempi per le Varie Categorie di Dati Personali (Art. 30(1)(2)(f) GDPR)	☐ Termini di legge o sino a revoca o diritto di opposizione ☐ Da contratto ☒ Termini di conservazione amministrativi
Sistemi IT e Applicativi	☒ Office automation su repository locali ☐ Office automation su cartelle in servizi in cloud ☐ Altre applicazioni
Localizzazione dei dati e dei supporti di backup	☒ Cartaceo In stanza Direzione presso sede in Piazza del Gesù e nell'archivio storico nei sotterranei ☒ Office automation su cartelle di file server Stanza Server presso sede in Piazza del Gesù, backup in loco ☐ Altre applicazioni

Attività di Trattamento: **Identificativo: Segreteria**	**indice N. 4:**
Data di inizio:	Data della modifica più recente:

Struttura organizzativa Punto di Contatto Telefono Indirizzo E-Mail (Art. 30(1)(2)(a) GDPR)	Direzione Generale e Segreteria Dott. Giorgio Tamaro
Finalità del trattamento (Art. 30(1)(2)(b) GDPR)	Gestione attività di supporto e documentazione del Consiglio di Amministrazione, dell'Assemblea dei Soci, del Collegio dei Sindaci Revisori dei Conti, dell'Organismo di Vigilanza L. 231 e del Comitato di Direzione, di tutti i Comitati, le Commissioni, le Consulte e i Gruppi di lavoro, anche costituiti ad hoc e in via temporanea, quali le Commissioni giudicatrici di gara e simili Assistenza alla Direzione, assistenza tecnica di primo livello agli attuatori dei Piani formativi finanziati, a supporto dell'Ufficio Formazione; gestione del servizio di helpdesk di primo livello verso i soggetti presentatori di Piani formativi a supporto dell'Ufficio Marketing.
Descrizione delle Categorie delle materie dei dati interessati (Art. 30(1)(2)(c) GDPR)	☒ Dipendenti ☐ Candidati ☒ Fornitori ☒ Soggetti attuatori ☐ Tirocinanti ☒ Consulenti ☒ Collaboratori ☐ Destinatari finali

Descrizione delle Categorie dei Dati Personali (Art. 30(1)(2)(c) GDPR)	☒ Personali identificativi ☐ ☐ Categorie Speciali di Dati Personali (Art. 9 e Art. 10 GDPR): ☐ Origine razziale o etnica ☐ Opinioni politiche ☐ Convinzioni religiose o filosofiche ☐ Appartenenza sindacale ☐ Vita sessuale o orientamento sessuale ☐ Genetici ☐ Biometrici ☐ Inerenti alla salute ☒ Provvedimenti giudiziari
Base Giuridica (Art 6 a/b/c/d/f)	a b c d e f ☐ ☒ ☐ ☐ ☐ ☐
	Informativa e modalità raccolta consenso

Categorie di Destinatari a cui i dati personali sono stati o saranno comunicati (Art. 30(1)(2)(d) GDPR)	Destinatari interni (Altre strutture che concorrono al trattamento) ☐ Direzione Generale e Segreteria ☒ Amministrazione ☒ Formazione ☒ Organizzazione ☒ Marketing ☒ Consiglio di Amministrazione ☐
	Destinatari Esterni (Categorie di Destinatari) ☒ Consulenti Fiscali, finanziari, legali e del lavoro ☐ Banche ☐ Istituti di assicurazione e previdenza ☐ Uffici delle imposte ☒ Collegio dei Revisori dei conti ☐ ☐ ☐
	Paesi terzi o Organizzazioni internazionali (Categorie) ☐ ☐ ☐ ☐

Se applicabile, Trasferimento di Dati Personali verso Paesi Terzi o Organizzazioni internazionali (Art. 30(1)(2)(e) GDPR) Identificazione dei Destinatari dei trasferimenti specifici	☒ Non si effettuano Trasferimenti e non sono previsti ☐ Trasferimenti che vengono effettuati sono i seguenti: ☐ Paesi terzi o Organizzazioni internazionali (identificare mediante nome)
A condizione che i Trasferimenti siano sottoposti alle disposizione dell' Art. 49(1) para. 2 GDPR [*Nota: Questi sono trasferimenti una tantum interessati da un "numero limitato" di individui considerati in base a "interessi legittimi impellenti"]:*	Documentazione delle garanzie sufficienti per i Trasferimenti
Conservazione/Eliminaz. e Tempi per le Varie Categorie di Dati Personali (Art. 30(1)(2)(f) GDPR)	☐ Termini di legge o sino a revoca o diritto di opposizione ☐ Da contratto ☒ Termini di conservazione amministrativi
Sistemi IT e Applicativi	☒ Office automation su repository locali ☐ Office automation su cartelle in servizi in cloud ☐ Altre applicazioni
Localizzazione dei dati e dei supporti di backup	☒ Cartaceo In stanza segreteria presso sede in Piazza del Gesù e nell'archivio storico nei sotterranei ☒ Office automation su cartelle di file server Stanza Server presso sede in Piazza del Gesù, backup in loco ☐ Altre applicazioni

3.2. Amministrazione

Di seguito sono descritti i processi con le informazioni e le modalità con cui i trattamenti sono operati:

Attività di Trattamento: **Identificativo: Contabilità e operazioni finanziarie**	**indice N. 5:**
Data di inizio:	Data della modifica più recente:

Struttura organizzativa Punto di Contatto Telefono Indirizzo E-Mail (Art. 30(1)(2)(a) GDPR)	Ufficio Amministrazione Dott.ssa Daniela Pengue
Finalità del trattamento (Art. 30(1)(2)(b) GDPR)	Gestione delle attività di tenuta della contabilità, cassa e banche, rilevazione delle entrate, pagamenti relativi alla gestione dell'ente, pagamenti di acconti e saldi delle attività formative finanziate, cura e conservazione delle pratiche di liquidazione di saldi ed acconti
Descrizione delle Categorie delle materie dei dati interessati (Art. 30(1)(2)(c) GDPR)	☐ Dipendenti ☐ Candidati ☒ Fornitori ☒ Soggetti attuatori ☐ Tirocinanti ☐ Consulenti ☐ Collaboratori ☐ Destinatari finali
Descrizione delle Categorie dei Dati Personali (Art. 30(1)(2)(c) GDPR)	☒ Personali identificativi ☐ ☐ Categorie Speciali di Dati Personali (Art. 9 e Art. 10 GDPR): ☐ Origine razziale o etnica ☐ Opinioni politiche ☐ Convinzioni religiose o filosofiche ☐ Appartenenza sindacale ☐ Vita sessuale o orientamento sessuale ☐ Genetici ☐ Biometrici ☐ Inerenti alla salute ☐ Provvedimenti giudiziari

Base Giuridica (Art 6 a/b/c/d/f)	a b c d e f ☐ ☒ ☐ ☐ ☐ ☐
	Informativa e modalità raccolta consenso Contratto
Categorie di Destinatari a cui i dati personali sono stati o saranno comunicati (Art. 30(1)(2)(d) GDPR)	Destinatari interni (Altre strutture che concorrono al trattamento) ☒ Direzione Generale e Segreteria ☐ Amministrazione ☐ Formazione ☐ Organizzazione ☐ Marketing ☒ Consiglio di Amministrazione ☐
	Destinatari Esterni (Categorie di Destinatari) ☒ Consulenti Fiscali, finanziari, legali e del lavoro ☒ Banche ☒ Istituti di assicurazione e previdenza ☐ Uffici delle imposte ☒ Collegio dei Revisori dei conti ☐ ☐ ☐
	Paesi terzi o Organizzazioni internazionali (Categorie) ☐ ☐ ☐ ☐

Se applicabile, Trasferimento di Dati Personali verso Paesi Terzi o Organizzazioni internazionali (Art. 30(1)(2)(e) GDPR) Identificazione dei Destinatari dei trasferimenti specifici	☒ Non si effettuano Trasferimenti e non sono previsti ☐ Trasferimenti che vengono effettuati sono i seguenti: ☐ Paesi terzi o Organizzazioni internazionali (identificare mediante nome)
A condizione che i Trasferimenti siano sottoposti alle disposizione dell' Art. 49(1) para. 2 GDPR [*Nota: Questi sono trasferimenti una tantum interessati da un "numero limitato" di individui considerati in base a "interessi legittimi impellenti"]:*	Documentazione delle garanzie sufficienti per i Trasferimenti
Conservazione/Eliminaz. e Tempi per le Varie Categorie di Dati Personali (Art. 30(1)(2)(f) GDPR)	☐ Termini di legge o sino a revoca o diritto di opposizione ☐ Da contratto ☒ Termini di conservazione amministrativi
Sistemi IT e Applicativi	☒ Office automation su repository locali ☐ Office automation su cartelle in servizi in cloud ☒ Altre applicazioni: software di contabilità Contabilità E
Localizzazione dei dati e dei supporti di backup	☒ Cartaceo In stanza Amministrazione presso sede in Piazza del Gesù e nell'archivio storico nei sotterranei ☒ Office automation su cartelle di file server Stanza Server presso sede in Piazza del Gesù, backup in loco ☒ Altre applicazioni Applicazione E presso Stanza Server in sede operativa in Piazza del Gesù, backup in loco

Attività di Trattamento: **Identificativo: Gestione Personale**	**indice N. 6:**
Data di inizio:	Data della modifica più recente:

Struttura organizzativa Punto di Contatto Telefono Indirizzo E-Mail (Art. 30(1)(2)(a) GDPR)	Ufficio Amministrazione Dott.ssa Daniela Pengue
Finalità del trattamento (Art. 30(1)(2)(b) GDPR)	Amministrazione del personale e gestione dei rapporti con il consulente del lavoro per gli adempimenti relativi;
Descrizione delle Categorie delle materie dei dati interessati (Art. 30(1)(2)(c) GDPR)	☒ Dipendenti ☒ Candidati ☐ Fornitori ☐ Soggetti attuatori ☐ Tirocinanti ☐ Consulenti ☒ Collaboratori ☐ Destinatari finali
Descrizione delle Categorie dei Dati Personali (Art. 30(1)(2)(c) GDPR)	☒ Personali identificativi ☐ ☐ Categorie Speciali di Dati Personali (Art. 9 e Art. 10 GDPR): ☐ Origine razziale o etnica ☐ Opinioni politiche ☐ Convinzioni religiose o filosofiche ☒ Appartenenza sindacale ☐ Vita sessuale o orientamento sessuale ☐ Genetici ☐ Biometrici ☒ Inerenti alla salute ☐ Provvedimenti giudiziari

Base Giuridica (Art 6 a/b/c/d/f)	a b c d e f ☐ ☒ ☐ ☐ ☐ ☐
	Informativa e modalità raccolta consenso Contratto
Categorie di Destinatari a cui i dati personali sono stati o saranno comunicati (Art. 30(1)(2)(d) GDPR)	Destinatari interni (Altre strutture che concorrono al trattamento) ☒ Direzione Generale e Segreteria ☐ Amministrazione ☐ Formazione ☐ Organizzazione ☐ Marketing ☒ Consiglio di Amministrazione ☐
	Destinatari Esterni (Categorie di Destinatari) ☒ Consulenti Fiscali, finanziari, legali e del lavoro ☐ Banche ☒ Istituti di assicurazione e previdenza ☒ Uffici delle imposte ☒ Medico Aziendale ☒ Collegio dei Revisori dei conti ☐ ☐
	Paesi terzi o Organizzazioni internazionali (Categorie) ☐ ☐ ☐ ☐

Se applicabile, Trasferimento di Dati Personali verso Paesi Terzi o Organizzazioni internazionali (Art. 30(1)(2)(e) GDPR) Identificazione dei Destinatari dei trasferimenti specifici	☒ Non si effettuano Trasferimenti e non sono previsti ☐ Trasferimenti che vengono effettuati sono i seguenti: ☐ Paesi terzi o Organizzazioni internazionali (identificare mediante nome)
A condizione che i Trasferimenti siano sottoposti alle disposizione dell' Art. 49(1) para. 2 GDPR [*Nota: Questi sono trasferimenti una tantum interessati da un "numero limitato" di individui considerati in base a "interessi legittimi impellenti"]:*	Documentazione delle garanzie sufficienti per i Trasferimenti
Conservazione/Eliminaz. e Tempi per le Varie Categorie di Dati Personali (Art. 30(1)(2)(f) GDPR)	☐ Termini di legge o sino a revoca o diritto di opposizione ☐ Da contratto ☒ Termini di conservazione amministrativi
Sistemi IT e Applicativi	☒ Office automation su repository locali ☐ Office automation su cartelle in servizi in cloud ☐ Altre applicazioni
Localizzazione dei dati e dei supporti di backup	☒ Cartaceo In stanza amministrazione presso sede in Piazza del Gesù e nell'archivio storico nei sotterranei ☒ Office automation su cartelle di file server Stanza Server presso sede in Piazza del Gesù, backup in loco ☐ Altre applicazioni

Attività di Trattamento: **Identificativo: Istruttorie di finanziamento**	**indice N. 7:**
Data di inizio:	Data della modifica più recente:

Struttura organizzativa Punto di Contatto Telefono Indirizzo E-Mail (Art. 30(1)(2)(a) GDPR)	Ufficio Amministrazione Dott.ssa Daniela Pengue
Finalità del trattamento (Art. 30(1)(2)(b) GDPR)	Gestione delle istruttorie di finanziamento dei Piani e Progetti formativi (controllo delle fideiussioni, gestione degli acconti e dei saldi, richieste di proroghe delle fidejussioni in scadenza per i Piani non integralmente conclusi dal punto di vista amministrativo e svincoli delle stesse in caso di piani con iter amministrativo completo); assistenza tecnica agli attuatori dei piani formativi in relazione alle richieste di chiarimenti e di informazioni sulle modalità di richiesta di acconti e saldi e sulle fidejussioni; assistenza tecnica agli operatori delle Articolazioni Regionali sulle pratiche amministrative;
Descrizione delle Categorie delle materie dei dati interessati (Art. 30(1)(2)(c) GDPR)	☐ Dipendenti ☐ Candidati ☐ Fornitori ☒ Soggetti attuatori ☐ Tirocinanti ☐ Consulenti ☐ Collaboratori ☐ Destinatari finali
Descrizione delle Categorie dei Dati Personali (Art. 30(1)(2)(c) GDPR)	☒ Personali identificativi ☐ ☐ Categorie Speciali di Dati Personali (Art. 9 e Art. 10 GDPR): ☐ Origine razziale o etnica ☐ Opinioni politiche ☐ Convinzioni religiose o filosofiche ☐ Appartenenza sindacale ☐ Vita sessuale o orientamento sessuale ☐ Genetici ☐ Biometrici ☐ Inerenti alla salute ☐ Provvedimenti giudiziari

Base Giuridica (Art 6 a/b/c/d/f)	a b c d e f ☐ ☒ ☐ ☐ ☐ ☐
	Informativa e modalità raccolta consenso
Categorie di Destinatari a cui i dati personali sono stati o saranno comunicati (Art. 30(1)(2)(d) GDPR)	Destinatari interni (Altre strutture che concorrono al trattamento) ☒ Direzione Generale e Segreteria ☐ Amministrazione ☐ Formazione ☒ Organizzazione ☒ Marketing ☒ Consiglio di Amministrazione ☐
	Destinatari Esterni (Categorie di Destinatari) ☐ Consulenti Fiscali, finanziari, legali e del lavoro ☐ Banche ☐ Istituti di assicurazione e previdenza ☐ Uffici delle imposte ☒ Collegio dei Revisori dei conti ☐ ☐ ☐
	Paesi terzi o Organizzazioni internazionali (Categorie) ☐ ☐ ☐ ☐

Se applicabile, Trasferimento di Dati Personali verso Paesi Terzi o Organizzazioni internazionali (Art. 30(1)(2)(e) GDPR) Identificazione dei Destinatari dei trasferimenti specifici	☒ Non si effettuano Trasferimenti e non sono previsti ☐ Trasferimenti che vengono effettuati sono i seguenti: ☐ Paesi terzi o Organizzazioni internazionali (identificare mediante nome)
A condizione che i Trasferimenti siano sottoposti alle disposizione dell' Art. 49(1) para. 2 GDPR [*Nota: Questi sono trasferimenti una tantum interessati da un "numero limitato" di individui considerati in base a "interessi legittimi impellenti"]:*	Documentazione delle garanzie sufficienti per i Trasferimenti
Conservazione/Eliminaz. e Tempi per le Varie Categorie di Dati Personali (Art. 30(1)(2)(f) GDPR)	☐ Termini di legge o sino a revoca o diritto di opposizione ☐ Da contratto ☒ Termini di conservazione amministrativi
Sistemi IT e Applicativi	☒ Office automation su repository locali ☐ Office automation su cartelle in servizi in cloud ☒ Altre applicazioni SIF e NSI
Localizzazione dei dati e dei supporti di backup	☒ Cartaceo In corridoio presso sede in Piazza del Gesù e nell'archivio storico nei sotterranei ☒ Office automation su cartelle di file server Stanza Server presso sede in Piazza del Gesù, backup in loco ☒ Altre applicazioni SIF e NSI presso Unidata con i relativi backup

Attività di Trattamento: **Identificativo: Contratti e approvvigionamenti**	**indice N. 8:**
Data di inizio:	Data della modifica più recente:

Struttura organizzativa Punto di Contatto Telefono Indirizzo E-Mail (Art. 30(1)(2)(a) GDPR)	Ufficio Amministrazione Dott.ssa Daniela Pengue
Finalità del trattamento (Art. 30(1)(2)(b) GDPR)	Gestione dei contratti in relazione alla stesura, cura e conservazione dei contratti disciplinanti i rapporti con fornitori di beni e servizi a qualsiasi titolo; acquisti e approvvigionamenti
Descrizione delle Categorie delle materie dei dati interessati (Art. 30(1)(2)(c) GDPR)	☐ Dipendenti ☐ Candidati ☒ Fornitori ☐ Soggetti attuatori ☐ Tirocinanti ☒ Consulenti ☒ Collaboratori ☐ Destinatari finali
Descrizione delle Categorie dei Dati Personali (Art. 30(1)(2)(c) GDPR)	☒ Personali identificativi ☐ ☐ Categorie Speciali di Dati Personali (Art. 9 e Art. 10 GDPR): ☐ Origine razziale o etnica ☐ Opinioni politiche ☐ Convinzioni religiose o filosofiche ☐ Appartenenza sindacale ☐ Vita sessuale o orientamento sessuale ☐ Genetici ☐ Biometrici ☐ Inerenti alla salute ☐ Provvedimenti giudiziari

Base Giuridica (Art 6 a/b/c/d/f)	a b c d e f ☐ ☒ ☐ ☐ ☐ ☐
	Informativa e modalità raccolta consenso Contratto
Categorie di Destinatari a cui i dati personali sono stati o saranno comunicati (Art. 30(1)(2)(d) GDPR)	Destinatari interni (Altre strutture che concorrono al trattamento) ☒ Direzione Generale e Segreteria ☐ Amministrazione ☐ Formazione ☐ Organizzazione ☐ Marketing ☒ Consiglio di Amministrazione ☐
	Destinatari Esterni (Categorie di Destinatari) ☒ Consulenti Fiscali, finanziari, legali e del lavoro ☒ Banche ☒ Istituti di assicurazione e previdenza ☐ Uffici delle imposte ☒ Collegio dei Revisori dei conti ☐ ☐ ☐
	Paesi terzi o Organizzazioni internazionali (Categorie) ☐ ☐ ☐ ☐

Se applicabile, Trasferimento di Dati Personali verso Paesi Terzi o Organizzazioni internazionali (Art. 30(1)(2)(e) GDPR) Identificazione dei Destinatari dei trasferimenti specifici	☒ Non si effettuano Trasferimenti e non sono previsti ☐ Trasferimenti che vengono effettuati sono i seguenti: ☐ Paesi terzi o Organizzazioni internazionali (identificare mediante nome)
A condizione che i Trasferimenti siano sottoposti alle disposizione dell' Art. 49(1) para. 2 GDPR [*Nota: Questi sono trasferimenti una tantum interessati da un "numero limitato" di individui considerati in base a "interessi legittimi impellenti"]:*	Documentazione delle garanzie sufficienti per i Trasferimenti
Conservazione/Eliminaz. e Tempi per le Varie Categorie di Dati Personali (Art. 30(1)(2)(f) GDPR)	☐ Termini di legge o sino a revoca o diritto di opposizione ☐ Da contratto ☒ Termini di conservazione amministrativi
Sistemi IT e Applicativi	☒ Office automation su repository locali ☐ Office automation su cartelle in servizi in cloud ☐ Altre applicazioni
Localizzazione dei dati e dei supporti di backup	☒ Cartaceo In stanza amministrazione presso sede in Piazza del Gesù e nell'archivio storico nei sotterranei ☒ Office automation su cartelle di file server Stanza Server presso sede in Piazza del Gesù, backup in loco ☒ Altre applicazioni

3.3. Formazione

Di seguito sono descritti i processi con le informazioni e le modalità con cui i trattamenti sono operati:

Attività di Trattamento: **Identificativo: Offerta formativa**	**indice N. 9:**
Data di inizio:	Data della modifica più recente:

Struttura organizzativa Punto di Contatto Telefono Indirizzo E-Mail (Art. 30(1)(2)(a) GDPR)	Ufficio Formazione Dott.ssa Tania Grandi
Finalità del trattamento (Art. 30(1)(2)(b) GDPR)	Gestione dei bandi ed helpdesk di 1° livello dei piani di formazione contenenti tutti i dati degli allievi e le convenzioni con gli enti contenenti i carichi pendenti, chiusura piani.
Descrizione delle Categorie delle materie dei dati interessati (Art. 30(1)(2)(c) GDPR)	☐ Dipendenti ☐ Candidati ☐ Fornitori ☒ Soggetti attuatori ☐ Tirocinanti ☐ Consulenti ☐ Collaboratori ☒ Destinatari finali
Descrizione delle Categorie dei Dati Personali (Art. 30(1)(2)(c) GDPR)	☒ Personali identificativi ☐ ☐ Categorie Speciali di Dati Personali (Art. 9 e Art. 10 GDPR): ☐ Origine razziale o etnica ☐ Opinioni politiche ☐ Convinzioni religiose o filosofiche ☐ Appartenenza sindacale ☐ Vita sessuale o orientamento sessuale ☐ Genetici ☐ Biometrici ☐ Inerenti alla salute ☒ Provvedimenti giudiziari

Base Giuridica (Art 6 a/b/c/d/f)	a b c d e f ☐ ☒ ☐ ☐ ☐ ☐
	Informativa e modalità raccolta consenso Contratto
Categorie di Destinatari a cui i dati personali sono stati o saranno comunicati (Art. 30(1)(2)(d) GDPR)	Destinatari interni (Altre strutture che concorrono al trattamento) ☒ Direzione Generale e Segreteria ☒ Amministrazione ☒ Formazione ☒ Organizzazione ☒ Marketing ☒ Consiglio di Amministrazione ☐
	Destinatari Esterni (Categorie di Destinatari) ☐ Consulenti Fiscali, finanziari, legali e del lavoro ☐ Banche ☐ Istituti di assicurazione e previdenza ☐ Uffici delle imposte ☒ Nucleo Tecnico di Valutazione ☒ Collegio dei Revisori dei conti ☐ ☐
	Paesi terzi o Organizzazioni internazionali (Categorie) ☐ ☐ ☐ ☐

Se applicabile, Trasferimento di Dati Personali verso Paesi Terzi o Organizzazioni internazionali (Art. 30(1)(2)(e) GDPR) Identificazione dei Destinatari dei trasferimenti specifici	☒ Non si effettuano Trasferimenti e non sono previsti ☐ Trasferimenti che vengono effettuati sono i seguenti: ☐ Paesi terzi o Organizzazioni internazionali (identificare mediante nome)
A condizione che i Trasferimenti siano sottoposti alle disposizione dell' Art. 49(1) para. 2 GDPR [*Nota: Questi sono trasferimenti una tantum interessati da un "numero limitato" di individui considerati in base a "interessi legittimi impellenti"]:*	Documentazione delle garanzie sufficienti per i Trasferimenti
Conservazione/Eliminaz. e Tempi per le Varie Categorie di Dati Personali (Art. 30(1)(2)(f) GDPR)	☐ Termini di legge o sino a revoca o diritto di opposizione ☐ Da contratto ☒ Termini di conservazione amministrativi
Sistemi IT e Applicativi	☒ Office automation su repository locali ☐ Office automation su cartelle in servizi in cloud ☒ Altre applicazioni: piattaforma informatica SIF e NSI
Localizzazione dei dati e dei supporti di backup	☒ Cartaceo In stanza Formazione presso sede in Piazza del Gesù e nell'archivio storico nei sotterranei ☒ Office automation su cartelle di file server Stanza Server presso sede in Piazza del Gesù, backup in loco ☒ Altre applicazioni SIF e NSI presso Unidata con i relativi backup

3.4. Organizzazione

Di seguito sono descritti i processi con le informazioni e le modalità con cui i trattamenti sono operati:

Attività di Trattamento: **Identificativo: Controllo piani formativi**	**indice N. 10:**
Data di inizio:	Data della modifica più recente:

Struttura organizzativa Punto di Contatto Telefono Indirizzo E-Mail (Art. 30(1)(2)(a) GDPR)	Ufficio Organizzazione Dott.ssa Maria Rita Evangelista
Finalità del trattamento (Art. 30(1)(2)(b) GDPR)	Supervisione delle procedure di controllo in itinere e finale dei Piani e Progetti finanziati svolte dalla Società esterna fornitrice del servizio; gestione delle pratiche relative ai controlli in itinere e finali (verbali di ispezione) e trasmissione all'Ufficio Amministrazione delle pratiche stesse per la liquidazione dei contributi; gestione delle procedure di rinunce, riparametrazioni e revoche dei Piani e Progetti finanziati; controllo dei rendiconti finali di spesa relativi alle attività delle Articolazioni Regionali e trasmissione all'Ufficio Amministrazione delle pratiche stesse per la liquidazione dei contributi; controllo dei rendiconti finali di spesa dei soggetti attuatori delle attività propedeutiche e trasmissione all'Ufficio Amministrazione delle pratiche stesse per la liquidazione dei contributi;
Descrizione delle Categorie delle materie dei dati interessati (Art. 30(1)(2)(c) GDPR)	☐ Dipendenti ☐ Candidati ☒ Fornitori ☒ Soggetti attuatori ☐ Tirocinanti ☐ Consulenti ☐ Collaboratori ☒ Destinatari finali

Descrizione delle Categorie dei Dati Personali (Art. 30(1)(2)(c) GDPR)	☒ Personali identificativi ☐ ☐ Categorie Speciali di Dati Personali (Art. 9 e Art. 10 GDPR): ☐ Origine razziale o etnica ☐ Opinioni politiche ☐ Convinzioni religiose o filosofiche ☐ Appartenenza sindacale ☐ Vita sessuale o orientamento sessuale ☐ Genetici ☐ Biometrici ☐ Inerenti alla salute ☒ Provvedimenti giudiziari
Base Giuridica (Art 6 a/b/c/d/f)	a b c d e f ☐ ☒ ☐ ☐ ☐ ☐
	Informativa e modalità raccolta consenso Contratto

Categorie di Destinatari a cui i dati personali sono stati o saranno comunicati (Art. 30(1)(2)(d) GDPR)	Destinatari interni (Altre strutture che concorrono al trattamento) ☒ Direzione Generale e Segreteria ☒ Amministrazione ☒ Formazione ☒ Organizzazione ☒ Marketing ☒ Consiglio di Amministrazione ☐
	Destinatari Esterni (Categorie di Destinatari) ☐ Consulenti Fiscali, finanziari, legali e del lavoro ☒ Banche ☒ Istituti di assicurazione e previdenza ☐ Uffici delle imposte ☒ Articolazioni Regionali ☒ Società di Auditing piani ☒ Collegio dei Revisori dei conti ☐
	Paesi terzi o Organizzazioni internazionali (Categorie) ☐ ☐ ☐ ☐

Se applicabile, Trasferimento di Dati Personali verso Paesi Terzi o Organizzazioni internazionali (Art. 30(1)(2)(e) GDPR) Identificazione dei Destinatari dei trasferimenti specifici	☒ Non si effettuano Trasferimenti e non sono previsti ☐ Trasferimenti che vengono effettuati sono i seguenti: ☐ Paesi terzi o Organizzazioni internazionali (identificare mediante nome)
A condizione che i Trasferimenti siano sottoposti alle disposizione dell' Art. 49(1) para. 2 GDPR [*Nota: Questi sono trasferimenti una tantum interessati da un "numero limitato" di individui considerati in base a "interessi legittimi impellenti"]:*	Documentazione delle garanzie sufficienti per i Trasferimenti
Conservazione/Eliminaz. e Tempi per le Varie Categorie di Dati Personali (Art. 30(1)(2)(f) GDPR)	☐ Termini di legge o sino a revoca o diritto di opposizione ☐ Da contratto ☒ Termini di conservazione amministrativi
Sistemi IT e Applicativi	☒ Office automation su repository locali ☐ Office automation su cartelle in servizi in cloud ☐ Altre applicazioni SIF e NSI
Localizzazione dei dati e dei supporti di backup	☒ Cartaceo Presso sede in Piazza del Gesù e nell'archivio storico nei sotterranei ☒ Office automation su cartelle di file server Stanza Server presso sede in Piazza del Gesù, backup in loco ☒ Altre applicazioni SIF e NSI presso Unidata con i relativi backup

Attività di Trattamento: **Identificativo: Piattaforme informatiche**	**indice N. 11:**
Data di inizio:	Data della modifica più recente:

Struttura organizzativa Punto di Contatto Telefono Indirizzo E-Mail (Art. 30(1)(2)(a) GDPR)	Ufficio Organizzazione Dott.ssa Maria Rita Evangelista
Finalità del trattamento (Art. 30(1)(2)(b) GDPR)	Supervisione della piattaforma informatica sviluppata e gestita dalla Società esterna fornitrice del servizio e rapporti con la Società stessa; referente per il funzionamento delle attrezzature informatiche (hardware e software) del Fondo;
Descrizione delle Categorie delle materie dei dati interessati (Art. 30(1)(2)(c) GDPR)	☒ Dipendenti ☒ Candidati ☒ Fornitori ☒ Soggetti attuatori ☐ Tirocinanti ☒ Consulenti ☒ Collaboratori ☒ Destinatari finali
Descrizione delle Categorie dei Dati Personali (Art. 30(1)(2)(c) GDPR)	☒ Personali identificativi ☐ ☐ Categorie Speciali di Dati Personali (Art. 9 e Art. 10 GDPR): ☐ Origine razziale o etnica ☐ Opinioni politiche ☐ Convinzioni religiose o filosofiche ☒ Appartenenza sindacale ☐ Vita sessuale o orientamento sessuale ☐ Genetici ☐ Biometrici ☒ Inerenti alla salute ☒ Provvedimenti giudiziari

Base Giuridica (Art 6 a/b/c/d/f)	a b c d e f ☒ ☒ ☐ ☐ ☐ ☐
	Informativa e modalità raccolta consenso Contratti e richiesta di consenso per finalità di Marketing
Categorie di Destinatari a cui i dati personali sono stati o saranno comunicati (Art. 30(1)(2)(d) GDPR)	Destinatari interni (Altre strutture che concorrono al trattamento) ☐ Direzione Generale e Segreteria ☐ Amministrazione ☐ Formazione ☐ Organizzazione ☐ Marketing ☐ Consiglio di Amministrazione ☐
	Destinatari Esterni (Categorie di Destinatari) ☐ Consulenti Fiscali, finanziari, legali e del lavoro ☐ Banche ☐ Istituti di assicurazione e previdenza ☐ Uffici delle imposte ☒ Fornitori ICT ☐ Collegio dei Revisori dei conti ☐ ☐
	Paesi terzi o Organizzazioni internazionali (Categorie) ☐ ☐ ☐ ☐

Se applicabile, Trasferimento di Dati Personali verso Paesi Terzi o Organizzazioni internazionali (Art. 30(1)(2)(e) GDPR) Identificazione dei Destinatari dei trasferimenti specifici	☒ Non si effettuano Trasferimenti e non sono previsti ☐ Trasferimenti che vengono effettuati sono i seguenti: ☐ Paesi terzi o Organizzazioni internazionali (identificare mediante nome)
A condizione che i Trasferimenti siano sottoposti alle disposizione dell' Art. 49(1) para. 2 GDPR [*Nota: Questi sono trasferimenti una tantum interessati da un "numero limitato" di individui considerati in base a "interessi legittimi impellenti"]:*	Documentazione delle garanzie sufficienti per i Trasferimenti
Conservazione/Eliminaz. e Tempi per le Varie Categorie di Dati Personali (Art. 30(1)(2)(f) GDPR)	☒ Termini di legge o sino a revoca o diritto di opposizione ☐ Da contratto ☒ Termini di conservazione amministrativi
Sistemi IT e Applicativi	☒ Office automation su repository locali ☐ Office automation su cartelle in servizi in cloud ☒ Altre applicazioni Directory server Active Directory Vmware per backup ambienti virtuali SIF e NSI
Localizzazione dei dati e dei supporti di backup	☐ Cartaceo Presso sede in Piazza del Gesù e nell'archivio storico nei sotterranei ☒ Office automation su cartelle di file server Stanza Server presso sede in Piazza del Gesù, backup in loco ☐

Attività di Trattamento: **Identificativo: Salute e Sicurezza**	**indice N. 12:**
Data di inizio:	Data della modifica più recente:

Struttura organizzativa Punto di Contatto Telefono Indirizzo E-Mail (Art. 30(1)(2)(a) GDPR)	Ufficio Organizzazione Dott.ssa Maria Rita Evangelista
Finalità del trattamento (Art. 30(1)(2)(b) GDPR)	Gestione delle pratiche relative al comparto sicurezza e salute della struttura interna del Fondo e rapporti con i consulenti esterni del servizio;
Descrizione delle Categorie delle materie dei dati interessati (Art. 30(1)(2)(c) GDPR)	☒ Dipendenti ☐ Candidati ☐ Fornitori ☐ Soggetti attuatori ☐ Tirocinanti ☐ Consulenti ☐ Collaboratori ☐ Destinatari finali
Descrizione delle Categorie dei Dati Personali (Art. 30(1)(2)(c) GDPR)	☒ Personali identificativi ☐ ☐ Categorie Speciali di Dati Personali (Art. 9 e Art. 10 GDPR): ☐ Origine razziale o etnica ☐ Opinioni politiche ☐ Convinzioni religiose o filosofiche ☐ Appartenenza sindacale ☐ Vita sessuale o orientamento sessuale ☐ Genetici ☐ Biometrici ☒ Inerenti alla salute ☐ Provvedimenti giudiziari

Base Giuridica (Art 6 a/b/c/d/f)	a b c d e f ☐ ☒ ☐ ☐ ☐ ☐
	Informativa e modalità raccolta consenso Contratto
Categorie di Destinatari a cui i dati personali sono stati o saranno comunicati (Art. 30(1)(2)(d) GDPR)	Destinatari interni (Altre strutture che concorrono al trattamento) ☒ Direzione Generale e Segreteria ☐ Amministrazione ☐ Formazione ☐ Organizzazione ☐ Marketing ☒ Consiglio di Amministrazione ☐
	Destinatari Esterni (Categorie di Destinatari) ☒ Consulenti Fiscali, finanziari, legali e del lavoro ☐ Banche ☒ Istituti di assicurazione e previdenza ☐ Uffici delle imposte ☒ Collegio dei Revisori dei conti ☐ ☐ ☐
	Paesi terzi o Organizzazioni internazionali (Categorie) ☐ ☐ ☐ ☐

Se applicabile, Trasferimento di Dati Personali verso Paesi Terzi o Organizzazioni internazionali (Art. 30(1)(2)(e) GDPR) Identificazione dei Destinatari dei trasferimenti specifici	☒ Non si effettuano Trasferimenti e non sono previsti ☐ Trasferimenti che vengono effettuati sono i seguenti: ☐ Paesi terzi o Organizzazioni internazionali (identificare mediante nome)
A condizione che i Trasferimenti siano sottoposti alle disposizione dell' Art. 49(1) para. 2 GDPR [*Nota: Questi sono trasferimenti una tantum interessati da un "numero limitato" di individui considerati in base a "interessi legittimi impellenti"]:*	Documentazione delle garanzie sufficienti per i Trasferimenti
Conservazione/Eliminaz. e Tempi per le Varie Categorie di Dati Personali (Art. 30(1)(2)(f) GDPR)	☐ Termini di legge o sino a revoca o diritto di opposizione ☐ Da contratto ☒ Termini di conservazione amministrativi
Sistemi IT e Applicativi	☒ Office automation su repository locali ☐ Office automation su cartelle in servizi in cloud ☐ Altre applicazioni
Localizzazione dei dati e dei supporti di backup	☐ Cartaceo Presso sede in Piazza del Gesù e nell'archivio storico nei sotterranei ☒ Office automation su cartelle di file server Stanza Server presso sede in Piazza del Gesù, backup in loco ☐ Altre applicazioni

3.5. Marketing, promozione e comunicazione, helpdesk

Di seguito sono descritti i processi con le informazioni e le modalità con cui i trattamenti sono operati:

Attività di Trattamento: **Identificativo: Liste Marketing e comunicazione**	**indice N. 13:**
Data di inizio:	Data della modifica più recente:

Struttura organizzativa Punto di Contatto Telefono Indirizzo E-Mail (Art. 30(1)(2)(a) GDPR)	Ufficio Marketing Dott. Giorgio Tamaro
Finalità del trattamento (Art. 30(1)(2)(b) GDPR)	Gestione dei rapporti con il territorio per la parte riguardante le attività di marketing, promozione e sviluppo. Gestione delle attività relative alla cura e supervisione del portale Fapi e della newsletter, incluso l'inserimento e l'aggiornamento delle informazioni sul sito del Fondo e la relativa gestione; organizzazione di convegni, manifestazioni e rapporti con la stampa.
Descrizione delle Categorie delle materie dei dati interessati (Art. 30(1)(2)(c) GDPR)	☐ Dipendenti ☐ Candidati ☐ Fornitori ☒ Soggetti attuatori e potenziali Soggetti attuatori ☐ Tirocinanti ☐ Consulenti ☐ Collaboratori ☐ Destinatari finali
Descrizione delle Categorie dei Dati Personali (Art. 30(1)(2)(c) GDPR)	☒ Personali identificativi ☐ ☐ Categorie Speciali di Dati Personali (Art. 9 e Art. 10 GDPR): ☐ Origine razziale o etnica ☐ Opinioni politiche ☐ Convinzioni religiose o filosofiche ☐ Appartenenza sindacale ☐ Vita sessuale o orientamento sessuale ☐ Genetici ☐ Biometrici ☐ Inerenti alla salute ☐ Provvedimenti giudiziari

Base Giuridica (Art 6 a/b/c/d/f)	a b c d e f ☒ ☐ ☐ ☐ ☐ ☐
	Informativa e modalità raccolta consenso Cartaceo durante gli eventi
Categorie di Destinatari a cui i dati personali sono stati o saranno comunicati (Art. 30(1)(2)(d) GDPR)	Destinatari interni (Altre strutture che concorrono al trattamento) ☒ Direzione Generale e Segreteria ☐ Amministrazione ☐ Formazione ☐ Organizzazione ☐ Marketing ☒ Consiglio di Amministrazione ☐
	Destinatari Esterni (Categorie di Destinatari) ☐ Consulenti Fiscali, finanziari, legali e del lavoro ☐ Banche ☐ Istituti di assicurazione e previdenza ☐ Uffici delle imposte ☒ Collegio dei Revisori dei conti ☐ ☐ ☐
	Paesi terzi o Organizzazioni internazionali (Categorie) ☐ ☐ ☐ ☐

Se applicabile, Trasferimento di Dati Personali verso Paesi Terzi o Organizzazioni internazionali (Art. 30(1)(2)(e) GDPR) Identificazione dei Destinatari dei trasferimenti specifici	☒ Non si effettuano Trasferimenti e non sono previsti ☐ Trasferimenti che vengono effettuati sono i seguenti: ☐ Paesi terzi o Organizzazioni internazionali (identificare mediante nome)
A condizione che i Trasferimenti siano sottoposti alle disposizione dell' Art. 49(1) para. 2 GDPR [*Nota: Questi sono trasferimenti una tantum interessati da un "numero limitato" di individui considerati in base a "interessi legittimi impellenti"]:*	Documentazione delle garanzie sufficienti per i Trasferimenti
Conservazione/Eliminaz. e Tempi per le Varie Categorie di Dati Personali (Art. 30(1)(2)(f) GDPR)	☒ Termini di legge o sino a revoca o diritto di opposizione ☐ Da contratto ☐ Termini di conservazione amministrativi
Sistemi IT e Applicativi	☒ Office automation su repository locali ☐ Office automation su cartelle in servizi in cloud ☐ Altre applicazioni
Localizzazione dei dati e dei supporti di backup	☒ Cartaceo Presso stanza Direzione sede in Piazza del Gesù e nell'archivio storico nei sotterranei ☒ Office automation su cartelle di file server Stanza Server presso sede in Piazza del Gesù, backup in loco ☐ Altre applicazioni

Attività di Trattamento: **Identificativo: Rapporti con l'INPS**	**indice N. 14:**
Data di inizio:	Data della modifica più recente:

Struttura organizzativa Punto di Contatto Telefono Indirizzo E-Mail (Art. 30(1)(2)(a) GDPR)	Ufficio Marketing Dott. Giorgio Tamaro
Finalità del trattamento (Art. 30(1)(2)(b) GDPR)	Gestione dei rapporti con l'INPS, soprattutto riguardo il data base delle iscrizioni, cancellazioni e controllo dei records degli iscritti;
Descrizione delle Categorie delle materie dei dati interessati (Art. 30(1)(2)(c) GDPR)	☐ Dipendenti ☐ Candidati ☐ Fornitori ☒ Soggetti attuatori e potenziali Soggetti attuatori ☐ Tirocinanti ☐ Consulenti ☐ Collaboratori ☒ Destinatari finali e potenziali destinatari
Descrizione delle Categorie dei Dati Personali (Art. 30(1)(2)(c) GDPR)	☒ Personali identificativi ☐ ☐ Categorie Speciali di Dati Personali (Art. 9 e Art. 10 GDPR): ☐ Origine razziale o etnica ☐ Opinioni politiche ☐ Convinzioni religiose o filosofiche ☐ Appartenenza sindacale ☐ Vita sessuale o orientamento sessuale ☐ Genetici ☐ Biometrici ☐ Inerenti alla salute ☐ Provvedimenti giudiziari

Base Giuridica (Art 6 a/b/c/d/f)	a b c d e f ☐ ☐ ☐ ☐ ☒ ☐
	Informativa e modalità raccolta consenso
Categorie di Destinatari a cui i dati personali sono stati o saranno comunicati (Art. 30(1)(2)(d) GDPR)	Destinatari interni (Altre strutture che concorrono al trattamento) ☒ Direzione Generale e Segreteria ☐ Amministrazione ☐ Formazione ☐ Organizzazione ☐ Marketing ☒ Consiglio di Amministrazione ☐
	Destinatari Esterni (Categorie di Destinatari) ☐ Consulenti Fiscali, finanziari, legali e del lavoro ☐ Banche ☐ Istituti di assicurazione e previdenza ☐ Uffici delle imposte ☒ Collegio dei Revisori dei conti ☐ ☐ ☐
	Paesi terzi o Organizzazioni internazionali (Categorie) ☐ ☐ ☐ ☐

Se applicabile, Trasferimento di Dati Personali verso Paesi Terzi o Organizzazioni internazionali (Art. 30(1)(2)(e) GDPR) Identificazione dei Destinatari dei trasferimenti specifici	☒ Non si effettuano Trasferimenti e non sono previsti ☐ Trasferimenti che vengono effettuati sono i seguenti: ☐ Paesi terzi o Organizzazioni internazionali (identificare mediante nome)
A condizione che i Trasferimenti siano sottoposti alle disposizione dell' Art. 49(1) para. 2 GDPR [*Nota: Questi sono trasferimenti una tantum interessati da un "numero limitato" di individui considerati in base a "interessi legittimi impellenti"]:*	Documentazione delle garanzie sufficienti per i Trasferimenti
Conservazione/Eliminaz. e Tempi per le Varie Categorie di Dati Personali (Art. 30(1)(2)(f) GDPR)	☒ Termini di legge o sino a revoca o diritto di opposizione ☐ Da contratto ☒ Termini di conservazione amministrativi
Sistemi IT e Applicativi	☒ Office automation su repository locali ☐ Office automation su cartelle in servizi in cloud ☐ Altre applicazioni
Localizzazione dei dati e dei supporti di backup	☐ Cartaceo ☒ Office automation su cartelle di file server Stanza Server presso sede in Piazza del Gesù, backup in loco ☐ Altre applicazioni

4. APPROCCIO BASATO SUL RISCHIO

4.1. Descrizione generale

L'approccio basato sul rischio è in primo luogo uno strumento efficace per garantire un elevato livello di protezione dei diritti e delle libertà delle persone. Consente a tutte le parti interessate di dedicare le proprie risorse alle aree in cui i rischi e i potenziali danni per le persone sono più significativi e per mitigare tali rischi. Questo a sua volta crea maggiori risultati e una più efficace protezione per le persone.

L'analisi dei rischi deve essere compiuta per ogni macro processo all'interno delle strutture organizzative, avendo attenzione alla tipologia degli eventi che possono generare danni e che comportano quindi rischi per la sicurezza dei dati personali, nonché all'impatto sui danni e sofferenze del cittadino interessato.

Una sfida chiave delle valutazioni del rischio sulla privacy è decidere quali rischi e danni ai singoli individui considerare, come pesarli e come valutare la probabilità e la gravità del danno.

Mentre il GDPR fornisce, in particolare nel suo *considerando* 75, orientamenti su ciò che è considerato rischioso o ad alto rischio, il presente Piano fornisce indicazioni di carattere generale senza entrare nel dettaglio dell'identificazione e della valutazione di rischi e danni particolari associati ai trattamenti dei dati.

Pertanto, parte della sfida nell'attuazione delle disposizioni sul rischio del GDPR consiste nel raggiungere una idonea valutazione sui rischi specifici e danni alle persone, che la gestione del rischio è destinato a identificare e mitigare. Questo è un primo passo fondamentale per ogni organizzazione.

Sono considerate ad alto rischio le aree nelle quali un accadimento, su uno più trattamenti all'interno dei processi, potrebbe produrre danni e sofferenze rilevanti e irreversibili nei confronti di cittadini quali soggetti interessati ed eventuali e conseguenti danni alla società.

L'articolo 24, paragrafo 1 richiede che i responsabili del trattamento applichino "gli opportuni requisiti tecnici e organizzativi con misure atte a garantire e dimostrare la conformità con il GDPR tenendo conto della "Natura, ambito, contesto e finalità del trattamento" e i rischi di varia natura e gravità per i diritti e le libertà delle persone.

Il responsabile del trattamento ha anche l'obbligo di rivedere e aggiornare tali misure "ove necessario".

Questa disposizione di responsabilità generale implica che un titolare deve costruire, implementare ed essere in grado di dimostrare un modello sulla privacy (ad esempio, leadership e supervisione, politiche e procedure, formazione e consapevolezza, monitoraggio e verifica, risposta e applicazione) in base a diversi fattori, compreso specificamente il livello di rischio per i diritti e le libertà fondamentali delle persone.

Ciò consentirà alle organizzazioni di calibrare o modulare il proprio programma di conformità in base ai rischi, danni e benefici per gli individui e per focalizzare la loro attenzione e le loro risorse per i trattamenti che creano "rischi" e "rischi elevati" per gli individui. Questo non assolve l'organizzazione dall'obbligo generale di conformità con il

GDPR in materia di elaborazione. Esso significa solo che i controlli effettivi, i passaggi di conformità e le verifiche saranno più intensi in relazione al trattamento che crea “rischi” o “rischi elevati” per i diritti fondamentali delle persone.

Ciò significa anche che gli attuali modelli di conformità alla privacy possono variare tra diversi organizzazioni basate sui vari livelli di rischio associati al loro trattamento.

Nell’ambito dei macroprocessi del prodotto/servizio e per ogni tipologia di rischio individuato verrà effettuata la valutazione. Ad ogni rischio individuato verrà associato un “peso” che consiste in un valore numerico (compreso tra 1 e 16), che fornirà informazioni sulla sua entità (basso, medio o alto).

4.2. Rischio e Alto Rischio nel GDPR

Il GDPR non definisce la nozione di "rischio", ma i *considerando* e le disposizioni includono indicazioni sui tipi di rischi e danni per gli individui che si devono considerare.

RISCHIO

	Descrizione
Definizione di rischio (Recital 75)	I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale (Recital 75)
Ulteriori esempi di rischio (Article 32.2)	• distruzione, perdita, modifica, divulgazione non autorizzata o accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati
Fattori da tenere conto quando si determina il livello di rischio (probabilità e gravità del rischio) (Recital 76)	• Natura; • Ambito di applicazione; • Contesto; • Finalità del trattamento
Rischio o Alto Rischio (Recital 76)	• Valutazione oggettiva

ALTO RISCHIO

	Descrizione
Quali tipi di trattamento possono risultare ad alto rischio?	• Ciascuno dei rischi può diventare "ad alto rischio", in base alla "probabilità e gravità" dei rischi determinati in un processo di valutazione del rischio in riferimento alla natura, all’ambito di applicazione, al contesto e alle finalità del trattamento;

	• quelli che comportano l'utilizzo di nuove tecnologie; • quelli che sono di nuovo tipo e in relazione ai quali il titolare del trattamento non ha ancora effettuato una valutazione d'impatto sulla protezione dei dati, o quando la valutazione d'impatto sulla protezione dei dati si riveli necessaria alla luce del tempo trascorso dal trattamento iniziale; • in particolare i trattamenti su larga scala, che mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati.

4.3. Alto Rischio e DPIA (WP248 rev.01)

Il GDPR non definisce la nozione di "rischio", ma secondo i *considerando* e la normativa, al fine di fornire un insieme più concreto insieme di operazioni di trattamento che richiedono un DPIA, a causa del loro elevato rischio intrinseco, tenendo conto degli elementi particolari dell'articolo 35 (1) e 35 (3) (a) - (c), l'elenco da adottare a livello nazionale ai sensi dell'articolo 35, paragrafo 4, e dei *considerando* 71, 75 e 91, nonché di altri riferimenti GDPR "suscettibili di rischio" operazioni di trattamento, possono essere considerati i seguenti nove criteri:

- **Valutazione o punteggio**, compresa la profilazione e la previsione, in particolare da "aspetti riguardanti le prestazioni del soggetto interessato sul luogo di lavoro, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o i movimenti" (punti 71 e 91).

- **Decisione automatizzata con significativo effetto giuridico o analogo**: trattamento che mira a prendere decisioni sugli interessati che producono "effetti giuridici riguardanti la persona fisica" o che "influenza in modo significativo anche la persona fisica" (articolo 35, paragrafo 3, lettera a)). Ad esempio, il trattamento può portare all'esclusione o alla discriminazione nei confronti degli individui.

- **Monitoraggio sistematico**: elaborazione utilizzata per osservare, monitorare o controllare le persone interessate, compresi i dati raccolti attraverso le reti o "un monitoraggio sistematico di un'area accessibile al pubblico" (articolo 35, paragrafo 3, lettera c).

- **Dati sensibili o dati di natura altamente personale**: ciò include categorie speciali di dati personali come definiti all'articolo 9 (ad esempio informazioni sulle opinioni politiche delle persone), nonché dati personali relativi a condanne penali o reati definiti all'articolo 10.

- **Dati trattati su larga scala**: il GDPR non definisce il concetto di larga scala, sebbene il *considerando* 91 fornisca alcune indicazioni. In ogni caso, il WP29

raccomanda che i seguenti fattori, in particolare, siano presi in considerazione per determinare se il trattamento è effettuato su larga scala:

- il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;
- il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;
- la durata, ovvero la persistenza, dell'attività di trattamento;
- la portata geografica dell'attività di trattamento.

- **Corrispondenza o combinazione di set di dati**, ad esempio provenienti da due o più operazioni di trattamento eseguite per scopi diversi e/o da diversi responsabili del trattamento dei dati in un modo che eccederebbe le ragionevoli aspettative dell'interessato.

- **Dati personali di persone fisiche vulnerabili** (*considerando* 75): il trattamento di questo tipo di dati è causa dell'aumento dello squilibrio di potere tra le persone interessate e il titolare del trattamento dei dati, il che significa che le persone potrebbero non essere in grado di acconsentire facilmente o opporsi al trattamento dei loro dati, o esercitare i loro diritti (bambini).

- **Uso innovativo o applicazione di nuove soluzioni tecnologiche o organizzative**, come la combinazione dell'uso di impronte digitali e riconoscimento facciale per un migliore controllo dell'accesso fisico, ecc.

- Quando il trattamento in sé "**impedisce agli interessati di esercitare un diritto o di utilizzare un servizio o un contratto**" (articolo 22 e *considerando* 91).

Nella maggior parte dei casi, un Titolare può considerare che un processo che soddisfa due criteri richiederebbe la realizzazione di una DPIA. In generale, il WP29 ritiene che più criteri sono soddisfatti in relazione al trattamento, maggiore è la probabilità di presentare un alto rischio per i diritti e le libertà degli interessati, e quindi di richiedere una DPIA, indipendentemente dalle misure che il Titolare prevede adottare.

4.4. Potenziali Minacce

La valutazione del rischio dovrebbe considerare le potenziali minacce di ogni processo di trattamento. Tali minacce includono:

- ingiustificabile o eccessiva raccolta di dati;
- uso o conservazione di dati obsoleti o inesatti;
- uso inappropriato o improprio dei dati, incluso l'uso di dati al di là della ragionevole aspettativa dell'individuo;
- perdita o distruzione di dati;
- alterazione dei dati;

- furto di dati;
- indisponibilità dei dati;
- ingiustificabile e non autorizzato accesso, trasferimento, condivisione o pubblicazione di dati.

4.5. Potenziali Danni

Le organizzazioni devono valutare la probabilità e gravità di qualsiasi danno che potrebbe risultare dai rischi di trattamento in relazione alle minacce che incombono su di essi. Tali danni possono includere:

a) Danni materiali, tangibili, fisici o economici all'individuo, come:

- danno fisico;
- perdita di libertà personale e di movimento;
- perdita finanziaria e di guadagno;
- altri significanti danni di interesse economico, per esempio causati da furto di identità.

b) Danni immateriali, intangibile sofferenza dell'individuo, come:

- danno derivante dal controllo o dall'esposizione di identità, caratteristiche, attività, associazioni o opinioni;
- limitazione della libertà di parola, associazione, ecc.;
- danno alla reputazione;
- incutere paura personale, familiare, lavorativa o sociale, imbarazzo, apprensione o ansia;
- inaccettabile intrusione nella vita privata;
- illecita discriminazione o stigmatizzazione;
- perdita di autonomia;
- limitazione della capacità personale di scelta;
- furto di identità e privazione del controllo sui dati personali.

5. VALUTAZIONE DEL RISCHIO

L’analisi viene solitamente effettuata per i macroprocessi all'interno di ciascun dipartimento organizzativo: in considerazione della struttura organizzativa del FAPI la valutazione del rischio verrà effettuata singolarmente a livello di ufficio. Ad ogni rischio identificato verrà associato un "peso" costituito da un valore numerico, che fornirà informazioni sulla sua entità. Il processo di valutazione del rischio sarà sviluppato in due fasi:

- Valutazione preliminare sulla probabile presenza di Alto Rischio che potrebbe causare elevati danni come specificato nel WP248;

- Valutazione delle potenziali minacce per il dipartimento raggruppando i processi di trattamento, per una individuazione del livello di rischio, che è determinato considerando la "probabilità" e la "gravità" dei rischi per l'individuo. "Probabilità" indica la probabilità che si concretizzi il rischio o l'impatto a fronte del rischio individuato, e "Gravità" indica l'entità del rischio o il suo impatto nel caso esso si materializzi.

5.1. Direzione Generale e Segreteria

	PROBABILITÀ DI ALTO RISCHIO	NOTE
☐	**Valutazione o punteggio**, compresa la profilazione e la previsione, in particolare da "aspetti riguardanti le prestazioni del soggetto interessato sul luogo di lavoro, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o i movimenti" (punti 71 e 91).	
☐	**Decisione automatizzata con significativo effetto giuridico o analogo**: trattamento che mira a prendere decisioni sugli interessati che producono "effetti giuridici riguardanti la persona fisica" o che "influenza in modo significativo anche la persona fisica" (articolo 35, paragrafo 3, lettera a). Ad esempio, il trattamento può portare all'esclusione o alla discriminazione nei confronti degli individui.	
☐	**Monitoraggio sistematico:** elaborazione utilizzata per osservare, monitorare o controllare le persone interessate, compresi i dati raccolti attraverso le reti o "un monitoraggio sistematico di un'area accessibile al pubblico" (articolo 35, paragrafo 3, lettera c).	
☒	**Dati sensibili o dati di natura altamente personale:** ciò include categorie speciali di dati personali come definiti all'articolo 9 (ad esempio informazioni sulle opinioni politiche delle persone), nonché dati personali relativi a condanne penali o reati definiti all'articolo 10.	Processi di trattamento per procedimenti legali
☐ ☐ ☐ ☐	**Dati trattati su larga scala:** il GDPR non definisce il concetto di larga scala, sebbene il *considerando* 91 fornisca alcune indicazioni. In ogni caso, il WP29 raccomanda che i seguenti fattori, in particolare, siano presi in considerazione per determinare se il trattamento è effettuato su larga scala: il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento; la durata, ovvero la persistenza, dell'attività di trattamento; la portata geografica dell'attività di trattamento. il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;	La struttura non effettua processi di trattamento su larga scala per le categorie di dati speciali sopra indicati.
☐	**Corrispondenza o combinazione di set di dati**, ad esempio provenienti da due o più operazioni di trattamento eseguite per scopi diversi e/o da diversi responsabili del trattamento dei dati in un modo che eccederebbe le ragionevoli aspettative dell'interessato	
☐	**Dati personali di persone fisiche vulnerabili** (*considerando* 75): il trattamento di questo tipo di dati è causa dell'aumento dello squilibrio di potere tra le persone interessate e il titolare del trattamento dei dati, il che significa che le persone potrebbero non essere in grado di acconsentire facilmente o opporsi trattamento dei loro dati, o esercitare i loro diritti (bambini)	
☐	**Uso innovativo o applicazione di nuove soluzioni tecnologiche o organizzative**, come la combinazione dell'uso di impronte digitali e riconoscimento facciale per un migliore controllo dell'accesso fisico, ecc.	
☐	Quando il trattamento in sé "**impedisce agli interessati di esercitare un diritto o di utilizzare un servizio o un contratto**" (articolo 22 e *considerando* 91).	

RISK MATRIX													
	Threats												
	Ingiustificabile o inaccurata raccolta			**Inappropriato o improprio uso dei dati**			**Violazione sui dati**			**Trasferimento di dati**			**Aggregato**
	Ingiustificabile o eccessiva raccolta di dati Uso o conservazione di dati inaccurati o obsoleti			Incluso l'uso di dati al di là della ragionevole aspettativa dell'individuo; Processi decisionali e ingiustificabili inferenze o deduzioni			Perdita di dati Furto di dati Violazione di accesso Indisponibilità dei dati			Ingiustificabile e non autorizzato accesso, trasferimento, condivisione o pubblicazione di dati			
	Likely Serious Score			**Likely Serious Score**			**Likely Serious Score**			**Likely Serious Score**			**Risk Rank**
Danni Tangibili													
Danno fisico	0	0	**0**	0	0	**0**	0	0	**0**	0	0	**0**	**0**
Perdita di libertà personale e di movimento	0	0	**0**	0	0	**0**	0	0	**0**	0	0	**0**	**0**
Perdita finanziaria	0	0	**0**	1	1	**2**	1	1	**4**	1	1	**0**	**6**
Altre perdite tangibili	0	0	**0**	0	0	**0**	0	0	**0**	0	0	**0**	**0**
Sofferenze Intangibili													
Eccessiva sorveglianza	0	0	**0**	0	0	**0**	0	0	**0**	0	0	**0**	**0**
Limitazione della libertà di parola, associazione, ecc	0	0	**0**	0	0	**0**	0	0	**0**	0	0	**0**	**0**
Danni reputazionali	0	0	**0**	0	0	**0**	0	0	**0**	0	0	**0**	**0**
Paura, imbarazzo e ansia	0	0	**0**	1	1	**2**	2	2	**4**	0	0	**0**	**6**
Discriminazione	0	0	**0**	0	0	**0**	0	0	**0**	0	0	**0**	**0**
Privazione di controllo sui dati personali	0	0	**0**	0	0	**0**	0	0	**0**	0	0	**0**	**0**

Punteggio "Probabilità/Gravità, 0 (n/a), 1 (bassa), 2 (media) 3 (alta)

Punteggio in base al rischio aggregato:
0- 8 Rischio non presente o basso rischio;
9-16 Rischio medio;
17-24 Alto Rischio.

5.2. Amministrazione

	PROBABILITÀ DI ALTO RISCHIO	NOTE
☐	**Valutazione o punteggio**, compresa la profilazione e la previsione, in particolare da "aspetti riguardanti le prestazioni del soggetto interessato sul luogo di lavoro, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o i movimenti" (punti 71 e 91).	
☐	**Decisione automatizzata con significativo effetto giuridico o analogo**: trattamento che mira a prendere decisioni sugli interessati che producono "effetti giuridici riguardanti la persona fisica" o che "influenza in modo significativo anche la persona fisica" (articolo 35, paragrafo 3, lettera a). Ad esempio, il trattamento può portare all'esclusione o alla discriminazione nei confronti degli individui.	
☐	**Monitoraggio sistematico:** elaborazione utilizzata per osservare, monitorare o controllare le persone interessate, compresi i dati raccolti attraverso le reti o "un monitoraggio sistematico di un'area accessibile al pubblico" (articolo 35, paragrafo 3, lettera c).	
☒	**Dati sensibili o dati di natura altamente personale:** ciò include categorie speciali di dati personali come definiti all'articolo 9 (ad esempio informazioni sulle opinioni politiche delle persone), nonché dati personali relativi a condanne penali o reati definiti all'articolo 10.	Dati inerenti la salute e l'appartenenza sindacale e casellari giudiziari.
☐	**Dati trattati su larga scala:** il GDPR non definisce il concetto di larga scala, sebbene il *considerando* 91 fornisca alcune indicazioni. In ogni caso, il WP29 raccomanda che i seguenti fattori, in particolare, siano presi in considerazione per determinare se il trattamento è effettuato su larga scala: ☐ il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento; ☐ la durata, ovvero la persistenza, dell'attività di trattamento; ☐ la portata geografica dell'attività di trattamento. ☐ il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;	La struttura non effettua processi di trattamento su larga scala per le categorie di dati speciali sopra indicati.
☐	**Corrispondenza o combinazione di set di dati**, ad esempio provenienti da due o più operazioni di trattamento eseguite per scopi diversi e/o da diversi responsabili del trattamento dei dati in un modo che eccederebbe le ragionevoli aspettative dell'interessato	
☐	**Dati personali di persone fisiche vulnerabili** (*considerando* 75): il trattamento di questo tipo di dati è causa dell'aumento dello squilibrio di potere tra le persone interessate e il titolare del trattamento dei dati, il che significa che le persone potrebbero non essere in grado di acconsentire facilmente o opporsi trattamento dei loro dati, o esercitare i loro diritti (bambini)	
☐	**Uso innovativo o applicazione di nuove soluzioni tecnologiche o organizzative**, come la combinazione dell'uso di impronte digitali e riconoscimento facciale per un migliore controllo dell'accesso fisico, ecc.	
☐	Quando il trattamento in sé "**impedisce agli interessati di esercitare un diritto o di utilizzare un servizio o un contratto**" (articolo 22 e *considerando* 91).	

RISK MATRIX													
	Threats												
	Ingiustificabile o inaccurata raccolta			**Inappropriato o improprio uso dei dati**			**Violazione sui dati**			**Trasferimento di dati**			**Aggregato**
	Ingiustificabile o eccessiva raccolta di dati Uso o conservazione di dati inaccurati o obsoleti			Incluso l'uso di dati al di là della ragionevole aspettativa dell'individuo; Processi decisionali e ingiustificabili inferenze o deduzioni			Perdita di dati Furto di dati Violazione di accesso Indisponibilità dei dati			Ingiustificabile e non autorizzato accesso, trasferimento, condivisione o pubblicazione di dati			
	Likely Serious Score			**Likely Serious Score**			**Likely Serious Score**			**Likely Serious Score**			**Risk Rank**
Danni Tangibili													
Danno fisico	0	0	**0**	0	0	**0**	0	0	**0**	0	0	**0**	**0**
Perdita di libertà personale e di movimento	0	0	**0**	0	0	**0**	0	0	**0**	0	0	**0**	**0**
Perdita finanziaria	0	0	**0**	1	1	**2**	1	2	**3**	1	2	**3**	**8**
Altre perdite tangibili	0	0	**0**	0	0	**0**	0	0	**0**	0	0	**0**	**0**
Sofferenze Intangibili													
Eccessiva sorveglianza	0	0	**0**	0	0	**0**	0	0	**0**	0	0	**0**	**0**
Limitazione della libertà di parola, associazione, ecc	0	0	**0**	0	0	**0**	0	0	**0**	0	0	**0**	**0**
Danni reputazionali	0	0	**0**	1	1	**2**	1	2	**3**	1	2	**3**	**8**
Paura, imbarazzo e ansia	0	0	**0**	1	1	**2**	1	2	**3**	1	2	**3**	**8**
Discriminazione	0	0	**0**	1	1	**2**	1	2	**3**	1	2	**3**	**6**
Privazione di controllo sui dati personali	0	0	**0**	1	1	**2**	1	2	**3**	1	2	**3**	**6**

Punteggio "Probabilità/Gravità, 0 (n/a), 1 (bassa), 2 (media) 3 (alta)

Punteggio in base al rischio aggregato:
0- 8 Rischio non presente o basso rischio;
9-16 Rischio medio;
17-24 Alto Rischio.

5.3. Formazione

	PROBABILITÀ DI ALTO RISCHIO	NOTE
☐	**Valutazione o punteggio**, compresa la profilazione e la previsione, in particolare da "aspetti riguardanti le prestazioni del soggetto interessato sul luogo di lavoro, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o i movimenti" (punti 71 e 91).	
☐	**Decisione automatizzata con significativo effetto giuridico o analogo**: trattamento che mira a prendere decisioni sugli interessati che producono "effetti giuridici riguardanti la persona fisica" o che "influenza in modo significativo anche la persona fisica" (articolo 35, paragrafo 3, lettera a). Ad esempio, il trattamento può portare all'esclusione o alla discriminazione nei confronti degli individui.	
☐	**Monitoraggio sistematico:** elaborazione utilizzata per osservare, monitorare o controllare le persone interessate, compresi i dati raccolti attraverso le reti o "un monitoraggio sistematico di un'area accessibile al pubblico" (articolo 35, paragrafo 3, lettera c).	
☒	**Dati sensibili o dati di natura altamente personale:** ciò include categorie speciali di dati personali come definiti all'articolo 9 (ad esempio informazioni sulle opinioni politiche delle persone), nonché dati personali relativi a condanne penali o reati definiti all'articolo 10.	Dati inerenti i casellari giudiziari.
☐ ☐ ☒ ☒	**Dati trattati su larga scala:** il GDPR non definisce il concetto di larga scala, sebbene il *considerando* 91 fornisca alcune indicazioni. In ogni caso, il WP29 raccomanda che i seguenti fattori, in particolare, siano presi in considerazione per determinare se il trattamento è effettuato su larga scala: il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento; la durata, ovvero la persistenza, dell'attività di trattamento; la portata geografica dell'attività di trattamento. il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;	La struttura non effettua processi di trattamento su larga scala per le categorie di dati speciali sopra indicati. Sono processati su larga scala solo dati comuni
☐	**Corrispondenza o combinazione di set di dati**, ad esempio provenienti da due o più operazioni di trattamento eseguite per scopi diversi e/o da diversi responsabili del trattamento dei dati in un modo che eccederebbe le ragionevoli aspettative dell'interessato	
☐	**Dati personali di persone fisiche vulnerabili** (*considerando* 75): il trattamento di questo tipo di dati è causa dell'aumento dello squilibrio di potere tra le persone interessate e il titolare del trattamento dei dati, il che significa che le persone potrebbero non essere in grado di acconsentire facilmente o opporsi trattamento dei loro dati, o esercitare i loro diritti (bambini)	
☐	**Uso innovativo o applicazione di nuove soluzioni tecnologiche o organizzative**, come la combinazione dell'uso di impronte digitali e riconoscimento facciale per un migliore controllo dell'accesso fisico, ecc.	
☐	Quando il trattamento in sé "**impedisce agli interessati di esercitare un diritto o di utilizzare un servizio o un contratto**" (articolo 22 e *considerando* 91).	

RISK MATRIX													
	Threats												
	Ingiustificabile o inaccurata raccolta			**Inappropriato o improprio uso dei dati**			**Violazione sui dati**			**Trasferimento di dati**			**Aggregato**
	Ingiustificabile o eccessiva raccolta di dati Uso o conservazione di dati inaccurati o obsoleti			Incluso l'uso di dati al di là della ragionevole aspettativa dell'individuo; Processi decisionali e ingiustificabili inferenze o deduzioni			Perdita di dati Furto di dati Violazione di accesso Indisponibilità dei dati			Ingiustificabile e non autorizzato accesso, trasferimento, condivisione o pubblicazione di dati			
	Likely Serious Score			**Likely Serious Score**			**Likely Serious Score**			**Likely Serious Score**			**Risk Rank**
Danni Tangibili													
Danno fisico	0	0	**0**	0	0	**0**	0	0	**0**	0	0	**0**	**0**
Perdita di libertà personale e di movimento	0	0	**0**	0	0	**0**	0	0	**0**	0	0	**0**	**0**
Perdita finanziaria	0	0	**0**	1	1	**2**	1	2	**3**	1	2	**3**	**8**
Altre perdite tangibili	0	0	**0**	0	0	**0**	0	0	**0**	0	0	**0**	**0**
Sofferenze Intangibili													
Eccessiva sorveglianza	0	0	**0**	0	0	**0**	0	0	**0**	0	0	**0**	**0**
Limitazione della libertà di parola, associazione, ecc	0	0	**0**	0	0	**0**	0	0	**0**	0	0	**0**	**0**
Danni reputazionali	0	0	**0**	1	1	**2**	1	2	**3**	1	2	**3**	**8**
Paura, imbarazzo e ansia	0	0	**0**	1	1	**2**	1	2	**3**	1	2	**3**	**6**
Discriminazione	0	0	**0**	0	0	**0**	0	0	**0**	0	0	**0**	**0**
Privazione di controllo sui dati personali	0	0	**0**	1	1	**2**	1	1	**2**	1	1	**2**	**6**

Punteggio "Probabilità/Gravità, 0 (n/a), 1 (bassa), 2 (media) 3 (alta)

Punteggio in base al rischio aggregato:
0- 8 Rischio non presente o basso rischio;
9-16 Rischio medio;
17-24 Alto Rischio.

5.4. Organizzazione

	PROBABILITÀ DI ALTO RISCHIO	NOTE
☐	**Valutazione o punteggio**, compresa la profilazione e la previsione, in particolare da "aspetti riguardanti le prestazioni del soggetto interessato sul luogo di lavoro, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o i movimenti" (punti 71 e 91).	
☐	**Decisione automatizzata con significativo effetto giuridico o analogo**: trattamento che mira a prendere decisioni sugli interessati che producono "effetti giuridici riguardanti la persona fisica" o che "influenza in modo significativo anche la persona fisica" (articolo 35, paragrafo 3, lettera a). Ad esempio, il trattamento può portare all'esclusione o alla discriminazione nei confronti degli individui.	
☐	**Monitoraggio sistematico:** elaborazione utilizzata per osservare, monitorare o controllare le persone interessate, compresi i dati raccolti attraverso le reti o "un monitoraggio sistematico di un'area accessibile al pubblico" (articolo 35, paragrafo 3, lettera c).	
☒	**Dati sensibili o dati di natura altamente personale:** ciò include categorie speciali di dati personali come definiti all'articolo 9 (ad esempio informazioni sulle opinioni politiche delle persone), nonché dati personali relativi a condanne penali o reati definiti all'articolo 10.	Dati inerenti la salute, l'appartenenza sindacale e casellari giudiziari.
☐ ☐ ☒ ☒	**Dati trattati su larga scala:** il GDPR non definisce il concetto di larga scala, sebbene il *considerando* 91 fornisca alcune indicazioni. In ogni caso, il WP29 raccomanda che i seguenti fattori, in particolare, siano presi in considerazione per determinare se il trattamento è effettuato su larga scala: il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento; la durata, ovvero la persistenza, dell'attività di trattamento; la portata geografica dell'attività di trattamento. il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;	La struttura non effettua processi di trattamento su larga scala per le categorie di dati speciali sopra indicati. Sono processati su larga scala solo dati comuni
☐	**Corrispondenza o combinazione di set di dati**, ad esempio provenienti da due o più operazioni di trattamento eseguite per scopi diversi e/o da diversi responsabili del trattamento dei dati in un modo che eccederebbe le ragionevoli aspettative dell'interessato	
☐	**Dati personali di persone fisiche vulnerabili** (*considerando* 75): il trattamento di questo tipo di dati è causa dell'aumento dello squilibrio di potere tra le persone interessate e il titolare del trattamento dei dati, il che significa che le persone potrebbero non essere in grado di acconsentire facilmente o opporsi trattamento dei loro dati, o esercitare i loro diritti (bambini)	
☐	**Uso innovativo o applicazione di nuove soluzioni tecnologiche o organizzative**, come la combinazione dell'uso di impronte digitali e riconoscimento facciale per un migliore controllo dell'accesso fisico, ecc.	
☐	Quando il trattamento in sé "**impedisce agli interessati di esercitare un diritto o di utilizzare un servizio o un contratto**" (articolo 22 e considerando 91).	

RISK MATRIX													
	Threats												
	Ingiustificabile o inaccurata raccolta			**Inappropriato o improprio uso dei dati**			**Violazione sui dati**			**Trasferimento di dati**			**Aggregato**
	Ingiustificabile o eccessiva raccolta di dati Uso o conservazione di dati inaccurati o obsoleti			Incluso l'uso di dati al di là della ragionevole aspettativa dell'individuo; Processi decisionali e ingiustificabili inferenze o deduzioni			Perdita di dati Furto di dati Violazione di accesso Indisponibilità dei dati			Ingiustificabile e non autorizzato accesso, trasferimento, condivisione o pubblicazione di dati			
	Likely Serious Score			**Likely Serious Score**			**Likely Serious Score**			**Likely Serious Score**			**Risk Rank**
Danni Tangibili													
Danno fisico	0	0	**0**	0	0	**0**	0	0	**0**	0	0	**0**	**0**
Perdita di libertà personale e di movimento	0	0	**0**	0	0	**0**	0	0	**0**	0	0	**0**	**0**
Perdita finanziaria	0	0	**0**	1	1	**2**	1	2	**3**	1	2	**3**	**8**
Altre perdite tangibili	0	0	**0**	0	0	**0**	0	0	**0**	0	0	**0**	**0**
Sofferenze Intangibili													
Eccessiva sorveglianza	0	0	**0**	0	0	**0**	0	0	**0**	0	0	**0**	**0**
Limitazione della libertà di parola, associazione, ecc	0	0	**0**	0	0	**0**	0	0	**0**	0	0	**0**	**0**
Danni reputazionali	0	0	**0**	1	1	**2**	1	2	**3**	1	2	**3**	**8**
Paura, imbarazzo e ansia	0	0	**0**	1	1	**2**	1	2	**3**	1	2	**3**	**6**
Discriminazione	0	0	**0**	1	1	**2**	1	1	**2**	1	1	**2**	**6**
Privazione di controllo sui dati personali	0	0	**0**	1	1	**2**	1	1	**2**	1	1	**2**	**6**

Punteggio "Probabilità/Gravità, 0 (n/a), 1 (bassa), 2 (media) 3 (alta)

Punteggio in base al rischio aggregato:
0- 8 Rischio non presente o basso rischio;
9-16 Rischio medio;
17-24 Alto Rischio.

5.5. Marketing, promozione e comunicazione, helpdesk

	PROBABILITÀ DI ALTO RISCHIO	NOTE
☐	**Valutazione o punteggio**, compresa la profilazione e la previsione, in particolare da "aspetti riguardanti le prestazioni del soggetto interessato sul luogo di lavoro, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o i movimenti" (punti 71 e 91).	
☐	**Decisione automatizzata con significativo effetto giuridico o analogo**: trattamento che mira a prendere decisioni sugli interessati che producono "effetti giuridici riguardanti la persona fisica" o che "influenza in modo significativo anche la persona fisica" (articolo 35, paragrafo 3, lettera a). Ad esempio, il trattamento può portare all'esclusione o alla discriminazione nei confronti degli individui.	
☐	**Monitoraggio sistematico:** elaborazione utilizzata per osservare, monitorare o controllare le persone interessate, compresi i dati raccolti attraverso le reti o "un monitoraggio sistematico di un'area accessibile al pubblico" (articolo 35, paragrafo 3, lettera c).	
☐	**Dati sensibili o dati di natura altamente personale:** ciò include categorie speciali di dati personali come definiti all'articolo 9 (ad esempio informazioni sulle opinioni politiche delle persone), nonché dati personali relativi a condanne penali o reati definiti all'articolo 10.	
☐ ☐ ☒ ☐	**Dati trattati su larga scala:** il GDPR non definisce il concetto di larga scala, sebbene il *considerando* 91 fornisca alcune indicazioni. In ogni caso, il WP29 raccomanda che i seguenti fattori, in particolare, siano presi in considerazione per determinare se il trattamento è effettuato su larga scala: il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento; la durata, ovvero la persistenza, dell'attività di trattamento; la portata geografica dell'attività di trattamento. il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;	La struttura effettua processi di trattamento unicamente su larga scala geografica che non implica un generale processo di larga scala. Sono inoltre processati solo dati comuni.
☐	**Corrispondenza o combinazione di set di dati**, ad esempio provenienti da due o più operazioni di trattamento eseguite per scopi diversi e/o da diversi responsabili del trattamento dei dati in un modo che eccederebbe le ragionevoli aspettative dell'interessato	
☐	**Dati personali di persone fisiche vulnerabili** (*considerando* 75): il trattamento di questo tipo di dati è causa dell'aumento dello squilibrio di potere tra le persone interessate e il titolare del trattamento dei dati, il che significa che le persone potrebbero non essere in grado di acconsentire facilmente o opporsi trattamento dei loro dati, o esercitare i loro diritti (bambini)	
☐	**Uso innovativo o applicazione di nuove soluzioni tecnologiche o organizzative**, come la combinazione dell'uso di impronte digitali e riconoscimento facciale per un migliore controllo dell'accesso fisico, ecc.	
☐	Quando il trattamento in sé "**impedisce agli interessati di esercitare un diritto o di utilizzare un servizio o un contratto**" (articolo 22 e *considerando* 91).	

RISK MATRIX													
	Threats												
	Ingiustificabile o inaccurata raccolta			**Inappropriato o improprio uso dei dati**			**Violazione sui dati**			**Trasferimento di dati**			**Aggregato**
	Ingiustificabile o eccessiva raccolta di dati Uso o conservazione di dati inaccurati o obsoleti			Incluso l'uso di dati al di là della ragionevole aspettativa dell'individuo; Processi decisionali e ingiustificabili inferenze o deduzioni			Perdita di dati Furto di dati Violazione di accesso Indisponibilità dei dati			Ingiustificabile e non autorizzato accesso, trasferimento, condivisione o pubblicazione di dati			
	Likely Serious Score			**Likely Serious Score**			**Likely Serious Score**			**Likely Serious Score**			**Risk Rank**
Danni Tangibili													
Danno fisico	0	0	**0**	0	0	**0**	0	0	**0**	0	0	**0**	**0**
Perdita di libertà personale e di movimento	0	0	**0**	0	0	**0**	0	0	**0**	0	0	**0**	**0**
Perdita finanziaria	0	0	**0**	0	0	**0**	0	0	**0**	0	0	**0**	**0**
Altre perdite tangibili	0	0	**0**	0	0	**0**	0	0	**0**	0	0	**0**	**0**
Sofferenze Intangibili													
Eccessiva sorveglianza	0	0	**0**	0	0	**0**	0	0	**0**	0	0	**0**	**0**
Limitazione della libertà di parola, associazione, ecc	0	0	**0**	0	0	**0**	0	0	**0**	0	0	**0**	**0**
Danni reputazionali	0	0	**0**	0	0	**0**	0	0	**0**	0	0	**0**	**0**
Paura, imbarazzo e ansia	0	0	**0**	0	0	**0**	0	0	**0**	0	0	**0**	**0**
Discriminazione	0	0	**0**	0	0	**0**	0	0	**0**	0	0	**0**	**0**
Privazione di controllo sui dati personali	0	0	**0**	1	1	**2**	1	1	**2**	1	1	**2**	**6**

Punteggio "Probabilità/Gravità, 0 (n/a), 1 (bassa), 2 (media) 3 (alta)

Punteggio in base al rischio aggregato:
0- 8 Rischio non presente o basso rischio;
9-16 Rischio medio;
17-24 Alto Rischio.

6. MISURE TECNICHE E ORGANIZZATIVE

Per misura si intende lo specifico intervento tecnico od organizzativo posto in essere (per prevenire, contrastare o ridurre gli effetti relativi ad una specifica minaccia), come pure quelle attività di verifica e controllo nel tempo, essenziali per assicurarne l'efficacia, che in sintesi possiamo indicare come:

- la pseudonimizzazione e la crittografia dei dati personali;
- la capacità di garantire la riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi di elaborazione;
- la possibilità di ripristinare la disponibilità e l'accesso ai dati personali in modo tempestivo in caso di incidente fisico o tecnico;
- un processo per testare, analizzare e valutare regolarmente l'efficacia di misure tecniche e organizzative per garantire la sicurezza dell'attività.

Di seguito il dettaglio delle misure tecniche e organizzative nel contesto di rischio (medio-basso):

6.1. Identificazione e Autenticazione degli utenti

Garantire che un utente acceda solo ai sistemi di cui ha bisogno: deve quindi essere associato a un unico identificatore e deve autenticarsi prima di qualsiasi accesso ai dati personali.

I fattori di autenticazione sono raggruppati in tre famiglie in base a:

- qualcosa che l'utente conosce, ad esempio una password;
- qualcosa che l'utente ha, ad esempio una smart card;
- qualcosa che l'utente fa, come ad esempio un'impronta digitale o una firma scritta a mano.

L'autenticazione di un utente è considerata forte quando richiede una combinazione di almeno due di questi fattori.

PRECAUZIONI DI BASE

- Definire un identificativo univoco per utente e vietare account condivisi tra più utenti. Nel caso in cui l'utilizzo di identificatori generici o condivisi è inevitabile, richiede una conferma esplicita da parte della direzione e attuare le misure per registrare le loro attività;
- Rispettare le raccomandazioni di base quando le password sono utilizzate per l'autenticazione, in particolare memorizzando il file password in modo sicuro e applicando a loro i seguenti requisiti di complessità:

  - avere una lunghezza di almeno 8 caratteri, compresi 3 tipi di caratteri su 4 (maiuscole, minuscole, numeri, caratteri speciali);

- Se l'autenticazione include una misura che limita l'accesso all'account come:
  - - blocco temporaneo dell'account dopo diversi tentativi falliti,
  - - un eventuale "Captcha",
  - - il blocco dell'account dopo 10 tentativi falliti;
  - - avere più di 5 caratteri se l'autenticazione richiede alcune informazioni riservate aggiuntive. Per le informazioni aggiuntive, utilizzare un identificatore riservato di almeno 7 caratteri e bloccare l'account al 5 ° tentativo fallito;
  - - la password può essere di soli 4 caratteri se l'autenticazione si basa sull'apparecchiatura posseduta dall'individuo e se la password viene utilizzata solo per sbloccare il dispositivo fisico detenuto dall'individuo stesso (ad esempio una smart card o un telefono cellulare) e che il dispositivo sia bloccato al 3 ° tentativo fallito.

I metodi mnemonici consentono di creare password complesse, ad esempio:

- usando solo la prima lettera delle parole in una frase;
- uppercasing se la parola è un nome (es .: C hief);
- mantenendo i segni di punteggiatura (es: ');
- esprimere numeri come cifre da 0 a 9 (es .: One 1).

Quando si accede per la prima volta, richiedere all'utente di modificare qualsiasi password attribuita da un amministratore o automaticamente dal sistema durante la creazione di un account, o reimpostare una password.

COSA SI DEVE EVITARE

- Comunicare la propria password a chiunque;
- Memorizzazione di password in un file non crittografato, su un foglio o in una posizione facilmente accessibile da altre persone;
- Salvataggio delle password nel browser senza utilizzare una password principale;
- Utilizzo di password con un collegamento a informazioni personali (nome, data di nascita, ecc.);
- Utilizzo della stessa password per accedere a diversi account;
- Mantenere la password predefinita;
- Invio di password personali tramite e-mail.

6.2. Gestione delle Autorizzazioni di accesso

Consentire solo l'accesso ai dati di cui l'utente ha realmente bisogno.

PRECAUZIONI DI BASE

- Definire i profili di autorizzazione nei sistemi separando le attività e l'area di responsabilità, al fine di limitare l'accesso degli utenti ai soli dati strettamente necessari per l'adempimento delle loro attività di trattamento in base alle loro responsabilità;

- Ritirare i diritti di accesso degli utenti non appena non sono più autorizzati ad accedere a una stanza o a una risorsa IT, ad esempio al termine del loro contratto;

- Effettuare una revisione annuale dei diritti di accesso al fine di identificare e rimuovere account non utilizzati e riallineare i diritti e il ruolo di ciascun utente.

COSA SI DEVE EVITARE

- Creazione o utilizzo di account condivisi per più utenti;

- Concessione dei diritti di amministratore agli utenti che non ne hanno bisogno;

- Concedere a un utente più privilegi del necessario;

- Dimenticare di rimuovere le autorizzazioni temporanee concesse a un utente (per una sostituzione, ad esempio);

- Dimenticare di cancellare gli account utente delle persone che hanno lasciato l'organizzazione o cambiato ruolo.

6.3. Tracciamento degli accessi e Gestione degli incidenti

Registrare l'accesso ai sistemi e organizzare le procedure di gestione degli incidenti, al fine di prendere le appropriate contromisure in caso di violazione sui dati (violazione di riservatezza, integrità o disponibilità).

Al fine di poter identificare l'accesso fraudolento o l' uso abusivo di dati personali, o per determinare l'origine di un incidente, è necessario registrare determinate azioni eseguite sui sistemi IT. Per fare questo, devono essere implementati dei sistemi di tracciamento con la registrazione dell'evento e le misure di gestione dell'incidente. Si devono registrare gli eventi rilevanti e garantire che questo registro non possa essere modificato. In ogni caso, questi elementi non devono essere conservati per un periodo di tempo eccessivo.

PRECAUZIONI DI BASE

- Configurare i tracciamenti (ovvero memorizzare gli eventi in "file di registro/log") per registrare le attività degli utenti, le anomalie e gli eventi relativi alla sicurezza:
    - - questi registri devono salvare eventi su un periodo che non può superare i sei mesi (tranne nel caso di un obbligo legale, o un rischio particolarmente significativo per gli interessati);
    - - come minimo, gli accessi devono essere registrati con il loro identificatore utente, la data e l'ora della loro connessione, nonché la data e l'ora della loro disconnessione;
    - - in alcuni casi, potrebbe essere necessario conservare anche informazioni sulle azioni intraprese dall'utente, la tipologia di dati consultati e / o modificati e il riferimento dei dati interessati.
- Informare gli utenti della presenza di un sistema di tracciamento, dopo aver informato e consultato il personale coinvolto;
- Proteggere le apparecchiature di tracciamento e le informazioni registrate da accessi non autorizzati, in particolare rendendole inaccessibili agli individui la cui attività è stata tracciata;
- Istituire procedure che effettuano il monitoraggio dei log e procedere periodicamente ad un monitoraggio per rilevare possibili anomalie;
- Assicurarsi che i responsabili della gestione dei sistemi di tracciamento comunichino al titolare dei dati, il prima possibile, qualsiasi anomalia o incidente di sicurezza;
- Notificare all'autorità di controllo competente per la protezione dei dati eventuali violazioni dei dati personali e, ad eccezione di indicazioni fornite dal GDPR, notificare anche alle persone interessate in caso di severo impatto, in modo che possano limitare le conseguenze della violazione.

COSA SI DEVE EVITARE

- Usare le informazioni provenienti dai log per un altro scopo, piuttosto che garantire l'uso corretto delle informazioni elaborazione (ad esempio: usare i registri per contare le ore lavorate è un uso improprio)

6.4. Sicurezza delle postazioni di lavoro

Prevenire l'accesso fraudolento, l'esecuzione di virus o l’acquisizione di controllo remoto, in particolare via Internet.

Sono da evitare i rischi di un'intrusione nei sistemi informatici: le workstation e i notebook sono uno dei punti principali di ingresso delle infrastrutture IT.

PRECAUZIONI DI BASE

- Implementare una procedura di disconnessione per bloccare qualsiasi workstation non utilizzata per un oltre un determinato periodo di tempo;
- Installare un firewall e limitare le porte di comunicazione autorizzate a quelle strettamente necessarie per il corretto funzionamento delle applicazioni installate sulle workstation;
- Utilizzare software antivirus regolarmente aggiornati e definire una politica che imponga aggiornamenti regolari dei software;
- Configurare i software in modo che gli aggiornamenti di sicurezza vengano eseguiti automaticamente quando possibile;
- Favorire la memorizzazione dei dati degli utenti su un supporto di memorizzazione regolarmente sottoposto a backup e accessibile tramite la rete dell’organizzazione piuttosto che sulle workstation stesse. Nel caso in cui i dati siano memorizzati localmente, fornire delle procedure di sincronizzazione o misure di backup per gli utenti e addestrarli nel loro uso;
- Limitare la connessione di supporti mobili (chiavette USB, dischi rigidi esterni, ecc.) all'essenziale;
- Disabilitare l'esecuzione automatica per i supporti rimovibili;
- Per assistenza temporanea sulle workstation attraverso strumenti di amministrazione remota, si devono eventualmente fornire delle credenziali temporanee prima di qualsiasi intervento se questo non viene svolto da amministratori di sistema preventivamente autorizzati.

COSA SI DEVE EVITARE

- Utilizzo di sistemi operativi obsoleti;
- Concessione dei diritti di amministratore agli utenti che non hanno competenze nella sicurezza IT.
- Esecuzione di applicazioni scaricate non provenienti da fonti sicure;
- Uso di applicazioni che richiedono diritti di amministratore.

6.5. Sicurezza dei dispositivi mobili

Evitare la violazione dei dati in seguito al furto o alla perdita di un'apparecchiatura mobile.

L'uso crescente di laptop, chiavette USB e smartphone rende necessaria la preparazione di misure per limitare la violazione dei dati, riducendo le probabilità di furto o la perdita di tali apparecchiature o l'accesso ai dati presenti.

PRECAUZIONI DI BASE

- Rendere consapevoli gli utenti sui rischi specifici associati all'uso di strumenti mobili (ad es. furto di attrezzature) e sulle procedure pianificate per ridurre questi rischi;
- Implementare misure di backup o sincronizzazione periodica per le workstation mobili, al fine di proteggersi contro la perdita dei dati memorizzati;
- Fornire misure di crittografia per proteggere le workstation mobili e i supporti di archiviazione mobile (laptop, penne USB, dischi rigidi esterni, CD-ROM, DVD-RW, ecc.), ad esempio:
    - - crittografia del disco rigido nella sua interezza quando il sistema operativo offre tale funzionalità;
    - - creazione di contenitori crittografati (un file contenente altri file e cartelle).
- Per quanto riguarda gli smartphone, oltre al codice PIN per la carta SIM, attivare il blocco automatico del terminale con la richiesta di informazioni confidenziali per sbloccarlo (password, schema, ecc.).

COSA SI DEVE EVITARE

- Utilizzo dei servizi cloud per il backup installati per impostazione predefinita, o effettuare la sincronizzazione senza eseguire un analisi approfondita delle loro condizioni d'uso e delle loro garanzie di sicurezza. Tali servizi non sono generalmente in grado di rispettare le misure fornite nella scheda da allegare/inserire al contratto della gestione dei subfornitori in subappalto.

6.6. Sicurezza dei server

Rafforzare le misure di sicurezza applicate ai server.

PRECAUZIONI DI BASE

- Consentire solo alle persone qualificate di accedere agli strumenti e alle interfacce di amministrazione, per assistenza temporanea sui server attraverso strumenti di amministrazione remota; si devono eventualmente fornire delle credenziali temporanee prima di qualsiasi intervento se questo non viene svolto da amministratori di sistema preventivamente autorizzati;

- Utilizzare account con minori privilegi per operazioni comuni;

- Adottare una politica password specifica per gli amministratori. Cambiare le password almeno ogni tre mesi per ogni sistema in gestione ad ogni singolo amministratore, centralizzando il sistema di identificazione;

- Installare gli aggiornamenti critici senza ritardi sia per i sistemi operativi che per le applicazioni, pianificando una verifica automatizzata settimanale;

- In termini di amministrazione del database:

  - - utilizzare identificativi di account personalizzati per accedere ai database e creare account specifici per ciascuna applicazione;

  - - implementare misure contro gli attacchi di SQL injection, script, ecc.

- Eseguire i backup e controllarli regolarmente;

- Implementare il protocollo TLS (in sostituzione di SSL 1) o un altro protocollo che garantisca la crittografia e l'autenticazione, come minimo per qualsiasi scambio di dati online e verificare la sua corretta implementazione tramite utilizzo di appropriati strumenti.

COSA SI DEVE EVITARE

- Utilizzo di servizi non protetti (autenticazione cleartext, flusso in chiaro, ecc.);

- Utilizzo di server che ospitano database per altre funzioni;

- Localizzazione di database su un server in una rete direttamente accessibile da Internet;

- Utilizzo di account utente generici (in altre parole condivisi tra più utenti).

6.7. Sicurezza dei siti Web

Garantire che le buone prassi di base vengano applicate ai siti Web.

Ogni sito web deve garantire l'integrità e la riservatezza delle informazioni che invia o raccoglie.

PRECAUZIONI DI BASE

- Implementare il protocollo TLS (che sostituisce SSL 23) su tutti i siti Web, utilizzando solo la versione più recente e controllare la sua corretta implementazione;
- Rendere obbligatorio l'uso di TLS per tutte le pagine, compresi i moduli che raccolgono dati personali o che autorizzano l'utente e quelli sui quali vengono visualizzati o trasmessi I dati personali non pubblici;
- Limitare le porte di comunicazione a quelle strettamente necessarie per il corretto funzionamento delle applicazioni installate. Se un server Web accetta solo connessioni HTTPS, solo il traffico di rete IP che entra in questa macchina sulla porta 443 deve essere autorizzato e tutte le altre porte devono essere bloccate;
- Consentire solo alle persone qualificate di accedere agli strumenti e alle interfacce di amministrazione. In particolare, limitare e profilare l'uso di account di amministratore agli amministratori di sistema solo per le azioni amministrative che lo richiedono;
- Se vengono utilizzati cookie non richiesti dal servizio, raccogliere il consenso dell'utente Internet dopo averlo informato e prima che il cookie sia depositato;
- Eseguire il monitoraggio del servizio WEB e mantenere aggiornati il software di base e i framework utilizzati.

COSA SI DEVE EVITARE

- Trasferimento di dati personali tramite una URL come ID o password;
- Utilizzo di servizi non protetti (autenticazione cleartext, flusso in chiaro, ecc.);
- Utilizzo di server che ospitano database o server come workstation, in particolare con client per la navigazione di siti Web, accesso elettronico messaggistica, ecc.;
- Localizzazione di database su un server direttamente accessibile da Internet;
- Utilizzo di account utente generici (in altre parole condivisi tra più utenti).

6.8. Protezione delle reti interne

Autorizzare solo le funzioni di rete necessarie per l'elaborazione dei trattamenti dei dati.

PRECAUZIONI DI BASE

- Limitare l'accesso a Internet bloccando i servizi non essenziali (VoIP, peer to peer, ecc.);
- Gestire le reti Wi-Fi. Devono utilizzare la crittografia avanzata (WPA2 o WPA2-PSK con password complesse) e le reti aperte agli ospiti devono essere separate dalla rete interna;
- Richiede una VPN per l'accesso remoto, nonché, se possibile, una autenticazione forte dell'utente (smart card, dispositivo di generazione password one-time “OTP”, ecc.);
- Assicurarsi che nessuna interfaccia di amministrazione sia direttamente accessibile da Internet. L’attività di manutenzione da remoto deve essere effettuata tramite una VPN;
- Limitare e filtrare il traffico di rete verso gli indirizzi IP e le porte TCP/UDP/ICMP/.. essenziali, filtrando il traffico in entrata e in uscita sull'apparecchiatura (firewall, proxy, server, ecc.). Ad esempio, se un server web utilizza HTTPS, si deve solo autorizzare il traffico in entrata verso questa macchina tramite la porta 443 e bloccare tutte le altre porte.

COSA SI DEVE EVITARE

- Utilizzo del protocollo telnet per la connessione remota alle apparecchiature di rete attive (firewall, router e switch). Invece, è consigliabile utilizzare SSH o un accesso fisico diretto all'apparecchiatura;
- Fornire agli utenti un accesso a Internet non filtrato;
- Configurazione di una rete Wi-Fi utilizzando una crittografia WEP.

6.9. Continuità del servizio

Effettuare backup regolari per evitare la perdita di dati e mantenere la loro integrità e definizione di un piano di ripristino dei dati per garantire la continuità del servizio

Le copie di backup devono essere eseguite e testate regolarmente. Deve essere preparato un piano di continuità operativa a fronte di possibili incidenti (ad es. guasto hardware, distruzione o manomissione dei dati anche involontaria).

PRECAUZIONI DI BASE

- Riguardo al backup dei dati:
  - - Eseguire backup periodici e frequenti dei dati, siano essi in formato cartaceo o elettronico. Potrebbe essere appropriato eseguire backup incrementali su base giornaliera e backup completi a intervalli regolari su periodo più lungo;
  - - Conservare i backup su un sito esterno, o se possibile in casseforti impermeabili e antincendio;
  - - Proteggere i dati di backup con lo stesso livello di sicurezza dei dati memorizzati sui server in produzione (ad esempio, crittografando i backup, organizzando l'archiviazione in un luogo sicuro o regolando contrattualmente un servizio di backup in outsourcing);
  - - Quando i backup vengono inviati tramite la rete, è consigliabile crittografare il loro canale di trasmissione se il trasporto non è svolto tra reti perimetrate all'interno della rete dell'organizzazione.
- Per quanto riguarda la gestione della continuità operativa:
  - - Creare un piano di gestione della continuità operativa dei servizi IT, anche se breve, includendo l'elenco delle persone coinvolte;
  - - Assicurarsi che utenti, fornitori di servizi e subappaltatori sappiano chi avvisare in caso di incidente;
  - - Testare periodicamente il ripristino dei backup e l'applicazione del piano di gestione della continuità operativa.
- Per quanto riguarda l'attrezzatura:
  - - utilizzare un gruppo di continuità per proteggere l’utilizzo della infrastruttura più critica;
  - - inserire la ridondanza dell'unità di memoria, ad esempio utilizzando una tecnologia RAID .

COSA SI DEVE EVITARE

- Mantenere i backup nello stesso luogo dei computer che ospitano i dati. Un grave incidente che si verificasse in questo luogo determinerebbe una perdita definitiva dei dati.

6.10. Sicurezza fisica

Rafforzare la sicurezza dei locali che ospitano le infrastrutture IT e le apparecchiature di rete.

L'accesso ai locali deve essere controllato per evitare o rallentare l'accesso non autorizzato, che si tratti di carta, file o apparecchiature IT, in particolare per i server.

PRECAUZIONI DI BASE

- Installare sistemi di allarme anti-intrusione e controllarli periodicamente;
- Installare rilevatori di fumo e strumenti antincendio e ispezionarli ogni anno;
- Garantire la sicurezza delle chiavi e dei codici di allarme che concedono l'accesso ai locali;
- Separare le aree dell'edificio in base ai rischi (ad esempio utilizzando un controllo di accesso dedicato per la sala computer);
- Tenere un elenco aggiornato delle persone o delle categorie di individui autorizzati a entrare in ciascuna area;
- Stabilire le regole e i metodi per controllare l'accesso dei visitatori, come minimo avere visitatori accompagnati, al di fuori delle aree di ricevimento pubbliche da una persona dell'organizzazione;
- Proteggere fisicamente le apparecchiature IT tramite metodi specifici (sistema di prevenzione incendi dedicato, attrezzatura di sollevamento contro possibili alluvioni, alimentazione elettrica e/o ridondanza del condizionamento d'aria, ecc.).

COSA SI DEVE EVITARE

- Trascurare la manutenzione delle sale computer (climatizzazione, UPS, ecc.): un guasto di questi sistemi spesso si traduce in macchine che si fermano o l'apertura di accesso alle camere (circolazione aria) che contribuiscono alla sicurezza fisica dei locali.

6.11. Sicurezza degli archivi storici

Assicurare l’archiviazione dei dati che non vengono più utilizzati su base giornaliera, ma che non hanno ancora raggiunto la fine del periodo di trattamento.

Gli archivi devono essere protetti, soprattutto se i dati archiviati sono dati sensibili o dati che potrebbero avere gravi conseguenze di impatto sugli interessati.

PRECAUZIONI DI BASE

- Definire una procedura di gestione degli archivi: quali dati devono essere archiviati, come e dove sono archiviati, come sono gestiti;

- Implementare metodi di accesso specifici ai dati archiviati, poiché l'uso di un archivio è realizzato in modo specifico ed eventualmente in modalità eccezionale;

- Per quanto riguarda la distruzione degli archivi, selezionare una procedura che garantisca che l'archivio sia stato distrutto nella sua interezza.

COSA SI DEVE EVITARE

- Utilizzo di supporti che non hanno una garanzia sufficiente in termini di longevità. Ad esempio, la longevità di CD e DVD riscrivibili raramente supera i quattro o cinque anni.

- Mantenere i dati in un database attivo semplicemente monitorando lo stato del servizio di dataserver o file server. I dati archiviati devono essere accessibili a un profilo specifico di incaricato.

6.12. Gestione del software e privacy by design and default

Integrare il prima possibile la sicurezza e la privacy nei progetti.

La privacy deve essere integrata nello sviluppo o modifiche dei servizi che coinvolgono modifiche o nuovi trattamenti di dati personali sin dalle fasi di progettazione, al fine di offrire ai soggetti interessati un migliore controllo sui propri dati e una limitazione di errori, perdite, modifiche non autorizzate o uso illecito di dati personali nelle applicazioni e infrastrutture tecnologiche coinvolte.

PRECAUZIONI DI BASE

- Integrare la privacy, compresi i requisiti di sicurezza, dalla progettazione di applicazioni o servizi. Questi requisiti possono influenzare le scelte di architettura (decentralizzata o centralizzata), caratteristiche (anonimizzazione, minimizzazione del dato), tecnologie (crittografia), ecc.;

- Per qualsiasi sviluppo che comporta trattamento di dati personali, esaminare i parametri relativi alla privacy, e in particolare la loro configurazione di default;

- Effettuare lo sviluppo del software e i test in un ambiente informatico separato dalla produzione (per esempio, su diversi computer o macchine virtuali) e utilizzare dati fittizi o resi anonimi.

COSA SI DEVE EVITARE

- Utilizzo di dati personali degli interessati nelle fasi di sviluppo e test. Dataset fittizi dovrebbero essere usati ogni volta che è possibile;

- Sviluppo di applicazioni o servizi senza tenere conto della sicurezza sui dati personali.

6.13. Crittografazione e autenticazione del dato

Garantire l'integrità, la riservatezza e l'autenticità del dato

Le funzioni di hash sono in grado di garantire l'integrità dei dati. Le Firme digitali, oltre a garantire l'integrità, sono in grado di verificare l'origine delle informazioni e la loro autenticità. Infine, la crittografia rende possibile garantire la riservatezza di un messaggio durante le fasi di conservazione e trasmissione.

PRECAUZIONI DI BASE

- Utilizzare un algoritmo riconosciuto e sicuro, ad esempio, i seguenti algoritmi:
    - - SHA-256, SHA-512 o SHA-3 come funzione hash;
    - - HMAC che utilizza SHA-256, bcrypt, scrypt o PBKDF2 per memorizzare le password;
    - - AES o AES-CBC per la crittografia simmetrica;
    - - RSA-OAEP come definito in PKCS # 1 v2.1 per la crittografia asimmetrica;
    - - infine, per le firme, RSA-SSA-PSS come specificato in PKCS # 1 v2.1.
- •.Utilizzare le dimensioni appropriate della chiave: per AES è consigliabile utilizzare chiavi di 128 bit e, per algoritmi basati su RSA, moduli ed esponenti segreti di almeno 2048 bit o 3072 bit, con esponenti pubblici, per la crittografia, maggiore di 65536;
- Proteggere le chiavi segrete, almeno con diritti di accesso restrittivi e una password sicura;
- Creare una procedura che descriva come gestire chiavi e certificati tenendo conto del caso di password dimenticate.

COSA SI DEVE EVITARE

- Utilizzo di algoritmi obsoleti, come DES e 3DES per la crittografia o MD5 e SHA1 come funzioni hash.
- Confondere una funzione di hash e un algoritmo di crittografia, o considerare che una funzione di hash è sufficiente per garantire la riservatezza dei dati. Sebbene le funzioni di hash siano funzioni "a senso unico", in altre parole funzioni che sono difficili da invertire, i dati possono talvolta essere recuperati dal suo hash. Queste funzioni sono in base alla progettazione, veloci da usare, quindi è solitamente possibile cancellare automaticamente tutti gli input possibili e quindi riconoscere l'output.

6.14. Gestione delle manutenzioni e distruzione dei dati

Garantire la sicurezza dei dati in ogni momento del ciclo di vita dell'hardware e software.

Le operazioni di manutenzione devono essere supervisionate per controllare l'accesso ai dati da parte dei fornitori di servizi. i dati devono essere distrutti prima di smaltire l'hardware.

PRECAUZIONI DI BASE

- Registrare la manutenzione e I rapportini di lavoro;
- Includere una clausola di sicurezza nei contratti di manutenzione stipulati dai fornitori di servizi;
- Assegnare a una persona la responsabilità dell'organizzazione di supervisionare il lavoro delle terze parti;
- Scrivere e implementare una procedura di cancellazione sicura dei dati;
- Cancellare in modo sicuro i dati dall'hardware prima che vengano smaltiti, inviati per la riparazione da una terza parte o al termine di un contratto di noleggio.

COSA SI DEVE EVITARE

- Installazione di applicazioni per la manutenzione remota con vulnerabilità note;
- Riutilizzo, rivendita o smaltimento di supporti contenenti dati personali cancellati.

6.15. Gestione dei Responsabili dei dati

Supervisionare la sicurezza dei dati con i fornitori dei servizi e i subfornitori.

I dati personali comunicati o gestiti dai responsabili dei dati e i subfornitori devono essere trattati fornendo e mantenendo garanzia dello stesso livello di sicurezza del titolare dei dati.

PRECAUZIONI DI BASE

- Utilizzare solo fornitori (Responsabili dei dati), con i relativi subfornitori, in grado di fornire sufficienti garanzie (in particolare in termini di specializzazione, conoscenza, affidabilità e risorse). Richiedere ai fornitori di servizi di comunicare la propria policy di sicurezza di gestione del sistema informativo prima di firmare un contratto;

- Prendere e documentare i mezzi (controlli di sicurezza, visite di installazione, ecc.) utilizzati per garantire l'efficacia delle garanzie offerte dal fornitore in termini di protezione dei dati. Queste garanzie includono:

    - - crittografia dei dati in base alla sua sensibilità o, almeno, all'esistenza di procedure che garantiscono che la società di servizi non ha visione dei dati più critici;

    - - crittografia delle trasmissioni di dati (es.: connessione di tipo HTTPS, VPN, ecc.);

    - - garanzie in termini di protezione della rete, tracciabilità (registri, audit), gestione dei diritti di accesso, autenticazione, ecc.

- Firmare un contratto con i fornitori , che definisce il soggetto, la lunghezza e lo scopo del programma di cessazione, così come gli obblighi di ciascuna parte. Assicurare che contenga, in particolare, disposizioni destinate a:

    - - il loro obbligo in termini di riservatezza dei dati personali affidati;

    - - standard minimi in termini di autenticazione dell'utente;

    - - condizioni di restituzione dei dati e/o della loro distruzione alla fine del contratto;

    - - gestione degli incidenti e regole di notifica. Dovrebbero includere la notifica del responsabile del trattamento dei dati di comunicare quanto prima se si scopre una violazione della sicurezza o un incidente di sicurezza.

COSA SI DEVE EVITARE

- Avvio del servizio di fornitura senza aver firmato un contratto con il responsabile dei dati, incluse le norme dell'articolo 28 del Regolamento sulla protezione dei dati;

- Utilizzo dei servizi di cloud computing in assenza di qualsiasi garanzia relativa all'efficacia geografica sulla posizione dei dati o senza garantire la liceità dei trasferimenti di dati al di fuori dell'Unione Europea e/o la necessità di ottenere un'autorizzazione dall’Autorità di controllo per procedere al trasferimento dei dati.

6.16. Sicurezza nello scambio dei dati con altre organizzazioni

Rafforzare la sicurezza in ogni trasmissione di dati personali.

I servizi di comunicazione elettronica non sono un mezzo di comunicazione sicuro per trasmettere dati personali, senza misure aggiuntive. Un semplice errore di gestione può comportare la divulgazione di dati personali a soggetti non autorizzati destinatari e quindi interferire con il diritto alla privacy delle persone. Inoltre, qualsiasi entità con accesso ai server interessati (in particolare quelli dei mittenti e dei destinatari) possono permettere di avere accesso ai loro contenuti.

PRECAUZIONI DI BASE

- Criptare i dati prima di inviarli su un supporto fisico (DVD, chiavetta USB, disco rigido portatile) ad una terza parte;
- Quando si inviano dati attraverso la rete:
  - - crittografare i documenti sensibili prima di inviarli;
  - - utilizzare un protocollo che garantisca la riservatezza e l'autenticazione del server destinatario per i trasferimenti di file, ad esempio SFTP o HTTPS, utilizzando la versione più recente dei protocolli.
  - - Garantire la riservatezza di informazioni riservate (chiavi di crittografia, password, ecc.) inviandoli tramite un canale separato (ad esempio, l'invio di un file crittografato tramite e-mail e la comunicazione della password per telefono o SMS);
- Se è necessario utilizzare un fax, impostare le seguenti misure:
  - - installare il fax in un luogo accessibile solo al personale autorizzato con controllo degli accessi fisici;
  - - visualizzare l'identità della macchina ricevente durante l'invio di messaggi;
  - - duplicare la trasmissione fax inviando anche i documenti originali al destinatario per posta;
  - - pre-registrare i potenziali destinatari nella rubrica della macchina del fax (quando questa funzione è disponibile).

COSA SI DEVE EVITARE

- Trasmissione di file contenenti dati personali non crittografati tramite generici pubblici provider di posta elettronica.

6.17. Piano di formazione

Rendere ciascun utente consapevole della necessità di mantenere la privacy e la sicurezza delle informazioni dell'organizzazione. Organizzare sessioni di sensibilizzazione, inviare regolarmente aggiornamenti sulle procedure pertinenti per i ruoli degli individui, inviare loro solleciti via e-mail, ecc.

PRECAUZIONI DI BASE

- Informare gli utenti delle misure attuate dalla loro organizzazione al fine di affrontare i rischi e le loro potenziali conseguenze.

- Documentare le procedure operative, tenerle aggiornate e renderle disponibili a tutti gli utenti interessati. In termini concreti, qualsiasi azione sui dati personali, sia che si tratti di operazioni legate all'amministrazione o di un semplice utilizzo di un'applicazione, deve essere spiegata in un linguaggio chiaro adattato a ciascuna categoria di utenti, in documenti a cui gli utenti possono fare riferimento.

- Spiegare il mansionario delle istruzioni IT (contenute anche nell'allegato A) e implementare la sua applicazione. Questo mansionario dovrebbe includere un promemoria delle regole di protezione dei dati e delle sanzioni subite in caso di inosservanza di queste regole e l'ambito di applicazione delle istruzioni indicate, che dovrebbe includere in particolare:

    - metodi di intervento dei team responsabili della gestione delle risorse IT per l'organizzazione;

    - mezzi di autenticazione utilizzati dall'organizzazione;

    - regole di sicurezza a cui gli utenti devono conformarsi, tra cui:

        - informare il dipartimento IT interno di qualsiasi sospetta violazione dei dati o di tentativi di violazione dell'account utente IT e in generale qualsiasi disfunzione;

        - mai affidare l'identificatore/password a terzi;

        - non installare, copiare, modificare o distruggere software senza autorizzazione;

        - bloccare i computer non appena gli utenti lasciano la postazione di lavoro;

        - non accedere mai, provare ad accedere o rimuovere informazioni se non si riferisce alle attività eseguite dall'utente;

        - rispettare le procedure definite in anticipo dalla società al fine di controllare il trasferimento dei dati sui media mobili, in particolare ottenendo un'autorizzazione preventiva da parte del supervisore e rispettando le norme di sicurezza.

        - rispettare le procedure definite in anticipo dalla società al fine di svolgere attività di emergenza di gestione del sistema nell'applicazione dei clienti che contiene i set di dati dell'utente finale.

    - Le procedure per l'utilizzo delle risorse informatiche e delle risorse di telecomunicazione disponibili per l'utente quali:

        - postazioni di lavoro;

        - apparecchiature mobili (specialmente nel contesto del telelavoro);

        - spazi di archiviazione individuali;

        - reti locali; dispositivi personali (in particolare le condizioni per utilizzare tali dispositivi);

        - la rete;

        - messaggistica elettronica;

        - telefonia.

    - Le condizioni per la gestione delle attività di amministrazione del sistema e, se necessario, l'esistenza di sistemi di filtraggio automatico e sistemi di registrazione automatica;

    - Responsabilità e sanzioni subite in caso di inosservanza delle istruzioni contenute nel mansionario.

7. TRATTAMENTI AFFIDATI ALL'ESTERNO

Rendendosi necessario l'affidamento di alcuni trattamenti di dati a soggetti esterni alla struttura, il FAPI, in qualità di Titolare del trattamento dei dati procede, in tale sezione del documento, a descrivere i soggetti Responsabili dei dati.
In particolare, la nomina dei soggetti è avvenuta per iscritto mediante apposita lettera nella quale, oltre che indicare l'attività esternalizzata, sono espressamente indicate le misure che il soggetto esterno si impegna a mettere in atto per garantire la sicurezza dei dati conformemente a quanto previsto dal Codice.
Il Titolare ha affidato l'attività a soggetti che forniscono i requisiti di affidabilità previsti nella normativa (EU) 679/16.

Di seguito, per ciascun soggetto responsabile identificato come "Outsourcer", vengono riportati:

- i dati identificativi;
- la natura e il trattamento dei dati esternalizzati.
- descrizione dell'attività;

Descrizione sintetica dell'attività esternalizzata	Trattamenti di dati interessati	Soggetto esterno
Nucleo tecnico di valutazione piani formativi	Visualizzazione	Alfiero Costantini Bruno Di Pietro Marco Laudani Maria Luisa Vignale Massimo Gentile Andrea Sonaglia
Controlli di rendicontazione con riferimento ai piani formativi finanziati	Visualizzazione	KRESTON GV ITALY AUDIT S.r.l.
Consulenza fiscale e del lavoro	Manutenzione, Conservazione e trasmissione dati e dei relativi backup	Studio Dottori Commercialisti Associati
Servizi ICT di sede operativa	Manutenzione, Conservazione e trasmissione dati e dei relativi backup	Paolo Santiangeli
Realizzazione Eventi e relativo supporto	Raccolta, visualizzazione	AIM ITALY S.r.l.
HelpDesk informativo e coordinamento e gestione di ogni aspetto riguardante le procedure informatiche	Visualizzazione	OOP SYSTEMS S.r.l.
Gestione di procedure informatiche del Fondo	Visualizzazione ed Estrazione	Fabio Calcopietro
Gestione Nuovo sistema informativo del fondo in SaaS (NSI)	Manutenzione, Conservazione e trasmissione dati e dei relativi backup	KAPUSONS S.rl. e STUDIO SAPERESSERE S.r.l.
Housing dei server contenenti Nuovo Sistema Informativo (NSI) e precedente Sistema informativo del fondo (SIF) e del Sistema informativo originario del Fondo SIO, backup e sicurezza perimetrale	Conservazione dati e dei relativi backup	Unidata SpA