DOCUMENTO GESTIONE PRIVACY

ai sensi del GDPR Reg. UE 2016/679
e del D.Lgs. 196/01
così come modificato dal D.Lgs. 101/18

INDICE

INTRODUZIONE 3

I DIRITTI DELL'INTERESSATO 10

L'ORGANIZZAZIONE 12

VALUTAZIONE D'IMPATTO DPIA 17

COVID 19 – GREEN PASS 26

CODICE DI CONDOTTA 27

INTRODUZIONE

Il **Regolamento generale per la protezione dei dati personali** n. 2016/679 (General Data Protection Regulation o **GDPR**) è la normativa di riforma della legislazione europea in materia di protezione dei dati. Pubblicato nella Gazzetta Ufficiale europea il 4 maggio 2016, è entrato in vigore il 24 maggio 2016, ma la sua attuazione (e quindi l'obbligo di applicazione) parte dal **25 maggio 2018**.
Trattandosi di un regolamento, non necessita di recepimento da parte degli Stati dell'Unione e viene attuato allo stesso modo in tutti gli Stati dell'Unione senza margini di libertà nell'adattamento. Il suo scopo è, infatti, la **definitiva armonizzazione della regolamentazione in materia di protezione dei dati personali all'interno dell'Unione europea**.

Il nuovo regolamento è più esplicito della direttiva 95/46 e supera la precedente legislazione italiana in materia di privacy (D.Lgs. 196/03) proclamando la tutela del **diritto alla protezione dei dati personali** inteso come **diritto fondamentale delle persone fisiche**. *Art. 1 par. 2 "Il presente regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali".*
In quest'ottica il principio cardine del nuovo regolamento è costituito dall'**autodeterminazione informativa**, condizione necessaria per il libero sviluppo della personalità del cittadino e anche un elemento essenziale di una società democratica.

Il nuovo regolamento europeo pone con particolare enfasi l'accento sulla **responsabilizzazione** del titolare e dei responsabili del trattamento, che si deve concretizzare nell'adozione di comportamenti proattivi a dimostrazione della concreta (e non meramente formale) adozione del regolamento. In particolare si evidenzia la necessità di attuare misure di tutela e garanzia dei dati trattati, con un approccio del tutto nuovo che **demanda ai titolari il compito di decidere autonomamente le modalità e i limiti del trattamento dei dati** alla luce dei criteri specifici indicati nel Regolamento:
- principio "*privacy by design*", in base al quale i prodotti e i servizi dovranno essere progettati fin dall'inizio in modo da tutelare la privacy degli utenti, cioè il trattamento deve essere previsto e configurato fin dall'inizio prevedendo le garanzie per tutelare i diritti degli interessati;
- rischio del trattamento, inteso come valutazione dell'impatto negativo sulle libertà e i diritti degli interessati.

L'approccio del GDPR è centrato su un approccio basato sulla valutazione del rischio (*risk based*), con il quale si determina la **misura di responsabilità del titolare o del responsabile del trattamento**, tenendo conto della natura, della portata, del contesto e delle finalità del trattamento, nonché della probabilità e della gravità dei rischi per i diritti e le libertà degli utenti. Un approccio *risk based* ha l'evidente vantaggio di pretendere degli obblighi che possono andare oltre la mera conformità alla legge, è sicuramente più flessibile e adattabile al mutare delle esigenze e degli strumenti tecnologici, ma ha anche lo svantaggio di **delegare all'azienda la valutazione del rischio**, rendendo più difficili le contestazioni in caso di violazioni. Le nuove norme prevedono, inoltre:

- per i cittadini un più facile accesso alle informazioni riguardanti i loro dati e le finalità e modalità di trattamento degli stessi;
- un diritto alla portabilità dei dati che consentirà di trasferire i dati personali tra i vari servizi online;
- l'istituzionalizzazione del diritto all'oblio (denominato diritto alla cancellazione nel regolamento) come previsto dalla Corte di Giustizia europea, che consentirà di chiedere ed ottenere la rimozione dei dati quando viene meno l'interesse pubblico alla notizia;
- l'obbligo di notifica da parte delle aziende delle gravi violazione dei dati dei cittadini; le aziende dovranno rispondere alla sola autorità di vigilanza dello Stato nel quale hanno la sede principale (principio del "*one stop shop*" o sportello unico);
- sanzioni amministrative fino al 4% del fatturato globale delle aziende in caso di violazioni delle norme.

Base giuridica del trattamento

Il nuovo regolamento pone l'accento sul **principio della trasparenza**, in un'ottica di rispetto della finalità. Occorre, quindi, valutare attentamente gli scopi del trattamento, in modo da stabilire correttamente quali dati possono essere trattati e quali no (principio di essenzialità dei dati).
Con il GDPR, inoltre, i titolari del trattamento dovranno identificare la base giuridica del trattamento (ad esempio il consenso dell'interessato) e documentarla, in quanto in relazione alla base giuridica possono variare i diritti. Ad esempio, è stato rafforzato il diritto alla cancellazione nel caso di trattamenti basati su consenso. Inoltre, la base giuridica è tra gli elementi essenziali dell'informativa e deve essere evidenziata in riscontro ad una istanza di accesso.

Trasparenza e conformità al regolamento

Il regolamento europeo prevede una serie di obblighi proattivi, a dimostrazione della concreta, e non meramente formale adozione del regolamento stesso. In tale ottica la

predisposizione e l'aggiornamento della documentazione è essenziale, in quanto indice di corretta implementazione delle norme:

- documentazione attestante i trattamenti svolti (registro dei trattamenti; valutazione di impatto, trasferimento dati extra UE);
- documentazione attestante il rispetto dei diritti degli interessati (informative, moduli raccolta consenso);
- documentazione di ripartizione ruoli e responsabilità (contratti e nomine dei responsabili esterni e autorizzati/incaricati; procedure interne, ecc...);
- documentazione attestante le misure di sicurezza implementate.

Ambito territoriale

Il Regolamento generale si applica ad ogni trattamento che ha ad oggetto dati personali, e a tutti i titolari (*controller*) e responsabili (*processor*) del trattamento stabiliti nel territorio dell'Unione, ma anche in generale a quelli che, offrendo beni e servizi a persone residenti nell'Unione, trattano dati di residenti nell'Unione europea (art. 3 del Regolamento).

In tal modo la sua applicazione non è limitata alle sole aziende che si trovano in Europa, ma tutela tutti gli interessati che risiedono nel territorio dell'Unione indipendentemente da dove si attua il trattamento dei loro dati.

Il regolamento, invece, non si applica nei seguenti casi:
- trattamenti effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione;
- trattamenti effettuati dagli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione del titolo V, capo 2, del Trattato dell'UE (politica estera e sicurezza);
- trattamenti effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse;
- trattamenti effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico.

Definizioni

«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;

«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;

«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;

«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;

«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;

«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;

«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;

«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;

«autorità di controllo»: l'autorità pubblica indipendente istituita da uno Stato membro;

Principi applicabili al trattamento dei dati personali

I dati personali sono:
a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, considerato incompatibile con le finalità iniziali («limitazione della finalità»);
c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);
e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);
f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:
a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;

d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso

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

I DIRITTI DELL'INTERESSATO

Il titolare del trattamento deve agevolare l'esercizio dei diritti da parte dell'interessato, adottando ogni misura (tecnica e organizzativa) a ciò idonea. **Il termine per la risposta all'interessato è, per tutti i diritti (compreso il diritto di accesso), 1 mese**, estendibili fino a 3 mesi in casi di particolare complessità; **il titolare deve comunque dare un riscontro all'interessato entro 1 mese dalla richiesta, anche in caso di diniego. Spetta al titolare** valutare la complessità del riscontro all'interessato e **stabilire l'ammontare dell'eventuale contributo** da chiedere all'interessato, ma soltanto se si tratta di richieste **manifestamente infondate o eccessive**, ovvero se sono chieste **più "copie" dei dati personali** nel caso del diritto di accesso; in quest'ultimo caso il titolare deve tenere conto dei costi amministrativi sostenuti. Il **riscontro all'interessato** di regola deve avvenire in **forma scritta** anche attraverso strumenti elettronici che ne favoriscano l'accessibilità; può essere dato **oralmente solo se così richiede l'interessato** stesso. La risposta fornita all'interessato non deve essere solo "intelligibile", ma anche **concisa, trasparente e facilmente accessibile**, oltre a utilizzare un **linguaggio semplice e chiaro**. **L'esercizio dei diritti è, in linea di principio, gratuito** per l'interessato, ma possono esservi eccezioni. Il titolare ha il diritto di chiedere informazioni necessarie a identificare l'interessato, e quest'ultimo ha il dovere di fornirle, secondo modalità idonee. Sono ammesse **deroghe ai diritti** riconosciuti dal regolamento, ma solo sul fondamento di disposizioni normative nazionali, ai sensi dell'articolo 23 nonché di altri articoli relativi ad ambiti specifici.

Diritto di accesso
Il diritto di accesso prevede **in ogni caso** il diritto di ricevere **una copia dei dati** personali oggetto di trattamento. Fra le informazioni che il titolare deve fornire **non rientrano le "modalità" del trattamento**, mentre **occorre indicare il periodo di conservazione** previsto o, se non è possibile, i criteri utilizzati per definire tale periodo, nonché le **garanzie** applicate **in caso di trasferimento dei dati verso Paesi terzi**.

Diritto alla cancellazione (oblio)
Il diritto cosiddetto "all'oblio" si configura come un diritto alla cancellazione dei propri dati personali in forma rafforzata. Si prevede, infatti, l'obbligo per i titolari (se hanno "reso pubblici" i dati personali dell'interessato: ad esempio, pubblicandoli su un sito web) **di informare della richiesta di cancellazione altri titolari che trattano i dati personali cancellati,** compresi "qualsiasi link, copia o riproduzione".

Diritto di limitazione del trattamento

È esercitabile **non solo in caso di violazione** dei presupposti di liceità del trattamento (quale alternativa alla cancellazione dei dati stessi), bensì anche **se l'interessato chiede la rettifica dei dati (in attesa di tale rettifica da parte del titolare**) o **si oppone al loro trattamento** ai sensi dell'art. 21 del regolamento (in attesa della valutazione da parte del titolare). Esclusa la conservazione, ogni altro trattamento del dato di cui si chiede la limitazione è vietato a meno che ricorrano determinate circostanze (consenso dell'interessato, accertamento diritti in sede giudiziaria, tutela diritti di altra persona fisica o giuridica, interesse pubblico rilevante).

Diritto alla portabilità dei dati

Non si applica ai trattamenti non automatizzati (quindi non si applica agli archivi o registri cartacei) e sono previste specifiche condizioni per il suo esercizio; in particolare, sono portabili **solo i dati trattati con il consenso dell'interessato o sulla base di un contratto stipulato con l'interessato** (quindi non si applica ai dati il cui trattamento si fonda sull'interesse pubblico o sull'interesse legittimo del titolare, per esempio), e solo i dati che siano stati **"forniti" dall'interessato** al titolare. Inoltre, il titolare deve essere in grado di trasferire direttamente i dati portabili a un altro titolare indicato dall'interessato, se tecnicamente possibile.

L'ORGANIZZAZIONE

AIAS ETS MILANO
sede legale e amministrativa via Paolo Mantegazza 10 20156 Milano
sede operativa via Paolo Mantegazza 10 20156 Milano
sede operativa piazza Comunale 21 20090 Pantigliate (MI)
sede operativa via Jannozzi 8 20097 San Donato Milanese (MI)
C.F. 80103190155 P.Iva 11408160155 REA CCIAA MI- 1666994
tel. 023302021 fax 02 33020250
mail amministrazione@aiasmilano.it web www.aiasmilano.it facebook aias di milano onlus

Da oltre 50 anni AIAS opera a Milano e hinterland per migliorare la salute e la qualità della vita delle persone con disabilità, di minori, adulti e anziani in situazioni di fragilità, promuovendone il benessere, l'autonomia e l'inclusione sociale, tramite i servizi erogati dalle aree sanitaria e sociale, per oltre 1500 utenti.

AIAS si rivolge principalmente a persone con disabilità nell'età evolutiva (da 0 a 18 anni) affette da patologie psicomotorie, psicoaffettive e da disturbi del neurosviluppo, senza dimenticare la fascia adulta. Per AIAS qualsiasi intervento riabilitativo non ha solo un carattere medico-sanitario ma deve valorizzare le capacità dell'individuo nella sua integrità, sensibilizzando allo stesso tempo l'ambiente esterno. Infatti all'interno di AIAS il concetto di riabilitazione assume un significato più

ampio, nel quale l'intervento medico si associa ad altri interventi, mirati allo sviluppo personologico dell'individuo e alla sua integrazione nella società. AIAS ha cominciato a raggiungere questo obiettivo realizzando una serie di servizi che, mettendo a punto un progetto condiviso da tutti i soggetti interessati (persone con disabilità, famiglie, operatori), accompagnino la persona nelle varie fasi della sua vita, rispondendo ai suoi bisogni e, nello stesso tempo, intervenendo sull'ambiente perché diventi accessibile e fruibile, in una prospettiva di inclusione.

In ambito socio sanitario AIAS è accreditata presso la Regione Lombardia come Istituto di Riabilitazione (ex art. 26 L. 833/78) operante nell'area dell'età evolutiva e dell'adulto con disabilità complessa. I servizi sanitari prevedono un percorso dalla diagnosi clinica e funzionale alla presa in carico con eventuale monitoraggio farmacologico. Le prestazioni dei servizi sanitari vengono erogate in regime ambulatoriale e domiciliare da personale specializzato altamente qualificato e in continuo aggiornamento formativo, sia in regime di convenzione con il sistema Sanitario, sia in solvenza.

In ambito sociale, il Servizio Progetti alla Persona di AIAS elabora, realizza e coordina progetti educativi, sia individualizzati sia di gruppo, per bambini, adolescenti e adulti su incarico di comuni, enti pubblici e famiglie, utilizzando educatori e altre figure professionali. Il servizio si occupa non solo di disabilità ma anche di integrazione sociale, di progetti nella scuola, di laboratori per le scuole e negli spazi extra scolastici, di sostegno a studenti con disabilità all'Università operando in ambito sociale a 360 gradi.

In ambito Formativo, AIAS, su indicazioni del Comitato Tecnico Scientifico interno all'Associazione, progetta una serie di proposte formative come occasione di riflessione e di confronto per molteplici figure professionali.

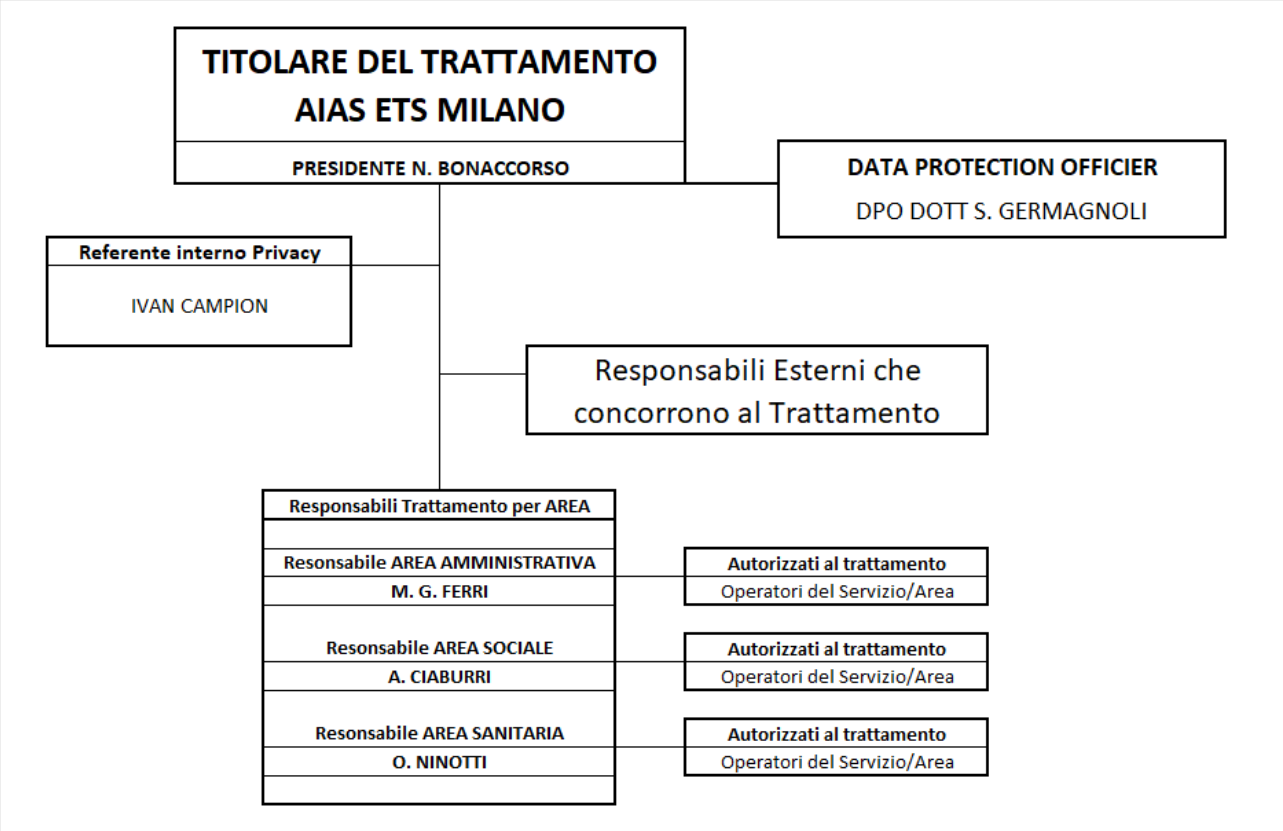
Ad oggi i Servizi e le Aree di intervento sono le seguenti:

- **Area Sanitaria**
  - Istituto di Riabilitazione in regime di accreditamento con Regione Lombardia
  - Istituto di Riabilitazione solventi

- **Area Socio-Educativa**
  - Educativa Scolastica
  - Domiciliarità
  - Centri Estivi
  - Progetti diversi

- **Area Formazione e Orientamento**
- Formazione
- Orientamento

Organigramma Privacy



Ruoli e funzioni Privacy

TITOLARE DEL TRATTAMENTO: è il Presidente e rappresentante legale dell'Associazione.
Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del regolamento europeo e tutelare i diritti degli interessati.
Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

RESPONSABILE DEL TRATTAMENTO: è nominato dal Titolare, qualora sia necessaria una ulteriore figura a garanzia delle operazioni di trattamento dei dati.
Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del regolamento europeo e garantisca la tutela dei diritti dell'interessato.
Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche.
I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento.

DATA PRIVACY OFFICER - DPO: è nominato dal Titolare a garanzia e tutela dei diritti delle persone interessate dal trattamento dei dati.
Il responsabile della protezione dei dati è incaricato almeno dei seguenti compiti:
a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal regolamento europeo nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
b) sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del

responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;
d) cooperare con l'autorità di controllo;

e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.
Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.
Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.
Il titolare e del trattamento e il responsabile del trattamento sostengono il responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'articolo 39 fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica.
Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti. Il responsabile della protezione dei dati non è rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti. Il responsabile della protezione dei dati riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento.
Gli interessati possono contattare il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal regolamento europeo.

REFERENTE PRIVACY INTERNO: è nominato dal Titolare quale supporto all'organizzazione nel trattamento dei dati. È responsabile per il presidio della compliance normativa e per l'aggiornamento, l'archiviazione e la gestione di tutta la documentazione dell'Associazione relativamente ai diversi aspetti privacy.

AUTORIZZATI/INCARICATI DEL TRATTAMENTO: sono nominati dal Titolare, sono tutti i Responsabili e gli Operatori che intervengono operativamente sul dato per utilizzarlo, analizzarlo, archiviarlo e comunicarlo.
L'autorizzato/incaricato è colui che effettua materialmente le operazioni di trattamento sui dati personali. Può essere solo una persona fisica, e deve agire sotto la diretta autorità del titolare del trattamento.

La nomina dell'autorizzato/incaricato deve avvenire con forma scritta, tramite atto nel quale sono indicati i nominativi e i compiti, compreso gli obblighi inerenti le misure di sicurezza. L'autorizzato/incaricato deve, ovviamente, attenersi strettamente alle istruzioni ricevute.

VALUTAZIONE D'IMPATTO DPIA

La **valutazione d'impatto sulla protezione dei dati** (**DPIA**, acronimo di "**Data Protection Impact Assessment**") è un processo che il titolare del trattamento deve effettuare quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche

L'**art. 35 del Regolamento europeo n. 2016/679** sulla protezione dei dati personali (GDPR) parla di valutazione d'impatto sulla protezione dei dati che deve essere effettuata dal titolare del trattamento quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche.
La valutazione contiene almeno:
a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, se del caso, l'interesse legittimo perseguito dal titolare del trattamento;
b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1;
d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Tipologia e natura dei dati trattati
AIAS raccoglie, gestisce, comunica e archivia una serie di dati personali e sensibili (sanitari e

giudiziari) relativi ai propri dipendenti e collaboratori, ai clienti pubblici e privati, ai committenti e ai fornitori, agli utenti dei servizi e alle loro famiglie. Relativamente ai dipendenti, ai soci, ai collaboratori, ai tirocinanti e ai volontari i dati sono dati personali e sensibili (nome e cognome, dati anagrafici, titolo di studio, esperienza lavorativa, coordinate bancarie, dati familiari, particolari condizioni di salute, particolari condizioni di reddito, certificato casellario giudiziale e dei carichi pendenti…) necessari alla gestione e alla tutela del contratto di lavoro o di collaborazione e dei rapporti sociali. Relativamente a clienti, committenti e fornitori i dati sono dati personali (anagrafica, coordinate bancarie…) necessari alla gestione dei contratti. Relativamente agli utenti dei servizi e alle loro famiglie i dati sono dati personali e sensibili (nome e cognome, dati anagrafici, dati familiari, condizione di salute, eventuali atti di natura giudiziaria come tutele, curatele, amministrazioni di sostegno, relazioni specialistiche e di altri servizi…); tali dati, peraltro richiesti in maniera vincolante dalle DGR che stabiliscono requisiti e criteri per le diverse unità di offerta e da convenzioni, contratti e accreditamenti, sono necessari ai fini dell'erogazione del servizio.

Categorie di interessati

AIAS ha determinato tre macro-categorie di soggetti interessati:

- dipendenti, soci, collaboratori, tirocinanti e volontari
- committenti e fornitori
- clienti/utenti e loro famiglie

Liceità e congruità del trattamento

Per quanto riguarda dipendenti, soci, collaboratori e volontari i dati vengono acquisiti e trattati sulla base di specifici vincoli contrattuali (Statuto dell'Associazione, leggi sul Terzo Settore, Contratto, lettere di incarico e contratti di consulenza, legislazione nazionale sul lavoro, DGR sulle diverse unità di offerta) con l'esclusiva finalità di gestione dei contratti di lavoro o di collaborazione e di gestione dei rapporti sociali all'interno dell'Associazione. Anche l'eventuale comunicazione a terzi di tali dati è strettamente legata a disposizioni di legge o a necessarie procedure di tipo contabile e amministrativo. Per quanto riguarda clienti pubblici e privati, committenti e fornitori i dati vengono acquisiti e trattati sulla base di specifici vincoli contrattuali (ordini e offerte, contratti, convenzioni, accreditamenti…) con l'esclusiva finalità di gestione dei contratti. Anche l'eventuale comunicazione a terzi di tali dati è strettamente legata a disposizioni di legge o a necessarie procedure di tipo contabile e amministrativo. Per quanto riguarda gli utenti dei servizi e le loro famiglie i dati vengono acquisiti e trattati sulla base di specifici vincoli legislativi (convenzioni e accreditamenti, DGR sulle diverse unità di offerta, contratti, leggi di settore…) con l'esclusiva finalità di gestire ed erogare in maniera efficace e corretta il servizio. Anche l'eventuale comunicazione a terzi di tali dati è strettamente legata a disposizioni di legge, vincoli derivanti da convenzioni e accreditamenti o a necessarie procedure di tipo contabile e amministrativo.

Descrizione del trattamento

Per il personale, i soci, i collaboratori e volontari i dati vengono raccolti e archiviati in formato cartaceo e/o elettronico ed eventualmente organizzati in database ordinati, in modo da poter espletare in maniera completa e corretta tutte le operazioni relative ai contratti e alle collaborazioni (operazioni sul contratto di lavoro, operazioni contabili e amministrative, adempimenti fiscali e assicurativi…). I dati raccolti possono essere consultati solo dal personale incaricato e preposto a tali operazioni e comunicate ai soggetti autorizzati o previsti per legge.
Per i clienti, i committenti e i fornitori, i dati vengono raccolti e archiviati in formato cartaceo e/o elettronico ed eventualmente organizzati in database ordinati, in modo da poter espletare in maniera completa e corretta tutte le operazioni relative ai contratti, alle convenzioni e agli accreditamenti (operazioni sui contratti, operazioni contabili e amministrative, adempimenti fiscali e assicurativi…). I dati raccolti possono essere consultati solo dal personale incaricato e preposto a tali operazioni e comunicate ai soggetti autorizzati o previsti per legge.
Per gli utenti e le loro famiglie i dati vengono raccolti e archiviati in formato cartaceo e/o elettronico ed eventualmente organizzati in cartelle e database ordinati, in modo da poter espletare in maniera completa e corretta tutte le operazioni relative all'erogazione del servizio (inserimento, osservazione, valutazione, presa in carico socio-educativa e socio-sanitaria, progettazione e verifica personalizzata, rapporti di rete, attività). I dati raccolti possono essere consultati solo dal personale incaricato e preposto a tali operazioni e comunicate ai soggetti autorizzati o previsti per legge.

Soggetti che eseguono il trattamento
AIAS ha provveduto a nominare formalmente gli incaricati al trattamento, specificando per ogni categoria di soggetti interessati, per tipologia di dati e per Area/Servizio le funzioni preposte al trattamento. Agli incaricati sono state fornite le necessarie istruzioni operative ed è stato loro consegnato il Codice di Condotta. AIAS ha provveduto inoltre a nominare i Responsabili interni ed esterni del trattamento e il DPO (Data Protection Officer).

Strumenti utilizzati per il trattamento
I dati vengono gestiti e archiviati sia in formato cartaceo che in formato elettronico.
Gli archivi cartacei sono costituiti da copie fotostatiche di documenti, dichiarazioni, attestazioni etc… e da stampe di file elaborati elettronicamente da programmi di scrittura o elaborazione del pacchetto Microsoft Office (Word, Excel). Alcuni dati contabili e amministrativi sono gestiti in formato elettronico da software gestionali dedicati
- Beatrix 2013
- Contas
- Arca Evolution (Wolters Kluver)

Cartelle e archivi cartacei sono riposti in armadi e classificatori in uffici chiusi con chiave.

Per quanto riguarda gli strumenti informatici l'Associazione dispone di:
- Unità Desktop PC

- Unità PC Portatili
- Unità Server

L'elenco completo degli strumenti elettronici, delle loro caratteristiche e della loro assegnazione è riportato in apposito elenco, documento archiviato e aggiornato dal Responsabile del trattamento.

Il Sistema Operativo è Microsoft Windows in diverse versioni (Windows 10, Windows 11), gli applicativi sono Microsoft Office.

La manutenzione hardware è in assistenza tramite garanzia dei produttori, oppure interna con la collaborazione esterna di Cbit srl tramite 'assistenza remota' senza accesso diretto ai sistemi AIAS.

È presente un firewall Watchguard T40 (Milano e Pantigliate) e T20 (San Donato) che:

- filtra la navigazione in uscita
- gestisce le NAT tra la rete interna e la navigazione internet
- gestisce la sicurezza della rete wireless: una per l'accesso alle risorse della rete Active Directory, l'altra per l'accesso degli ospiti con un indirizzo ip diverso dalla rete aziendale
- le VPN con le sedi esterne

L'antivirus installato è: Bitdefender

Firewall e antivirus si aggiornano automaticamente.

Gli aggiornamenti dei sistemi operativi vengono effettuati automaticamente, sia sui server sia sui client, a meno di falle definite ZERO DAY, che vengono installate appena Microsoft le mette a disposizione

Le password degli utenti vengono aggiornate automaticamente ogni 180 giorni tramite richiesta automatica predefinita nelle policy del Domain Controller 15 giorni prima della scadenza.

L'ora di sistema dei PC all'interno del dominio viene regolata da una policy predefinita sul Domain controller che verifica una volta al giorno la sincronizzazione dell'ora con un server NTP italiano (ntp1.inrim.it e ntp2.inrim.it).

Il Domain Controller Primario e Secondario gestisce inoltre il servizio DNS locale e il l'assegnazione degli ip dei dispositivi all'interno della rete primaria di AIAS ETS MILANO. L'accesso alla rete ospiti è regolata dal firewall sia come DNS che per assegnazione indirizzi IP

I backup sono giornalieri e vengono effettuati su NAS localmente tramite il programma VEEAM Backup & Replication che invia a fine procedura via email i risultati delle operazioni.

Sono presenti due gruppi di continuità gestiti per mantenere attivo i server e gli apparati di rete in caso di mancanza di corrente modello EATON 1360 con capacità di 2000VA e EATON 9E6Ki con capacità di 6000VA che verificano una volta alla settimana l'affidabilità delle batterie automaticamente e invia report via email.

Collocazione dei dati

Archivi cartacei in armadi situati nei luoghi di lavoro; computer situati all'interno dei luoghi di lavoro (Sede legale e sedi operative). Un elenco con l'attribuzione dei diversi PC (e degli eventuali archivi cartacei) è inserito nell'Elenco PC, documento archiviato e aggiornato dal Responsabile IT.

Strutture che concorrono al trattamento

Per il personale, i soci, i collaboratori e i volontari:

- Centro per l'elaborazione paghe
- Manutenzione Hardware e Software
- INPS, INAIL e altri enti statali di riferimento
- Agenzia delle Entrate
- Revisore/Collegio Sindacale
- Assicurazione
- RSPP
- Medico Competente
- Forze dell'ordine, di pubblica sicurezza e di pronto soccorso

Per clienti, committenti e fornitori

- Agenzia delle entrate
- Revisore

Per gli utenti e le loro famiglie

- Enti invianti
- Servizi Sociali
- ASST e relativi servizi e presidi
- Medici di base e specialisti
- Tutori, Curatori e Amministratori di Sostegno
- Servizi territoriali di riferimento
- Tribunali
- Forze dell'ordine e di pubblica sicurezza e di pronto soccorso

Analisi dei rischi

Rischi	**SI/NO**	**Descrizione dell'impatto sulla sicurezza *(gravità: alta, media, bassa)***
Comportamento degli operatori		
Sottrazione di credenziali di autenticazione	**SI**	Rischio furto dati. Gravità **Bassa**
Carenza di consapevolezza, disattenzione o incuria	**SI**	Rischio perdita dei dati. Gravità **Bassa**
Comportamenti sleali o fraudolenti	**SI**	Rischio furto dati. Gravità **Bassa**
Errore materiale	**SI**	Rischio perdita dati. Gravità **Media**
Eventi relativi agli strumenti		
Azione di virus informatici o di programmi suscettibili di recare danno	**SI**	Rischio danneggiamento o perdita dati. Gravità **Media**
Spamming o tecniche di sabotaggio	**SI**	Rischio danneggiamento, sottrazione o perdita dati. Gravità **Bassa**
Malfunzionamento, indisponibilità o degrado degli strumenti	**SI**	Rischio danneggiamento o perdita dati. Gravità **Bassa**
Accessi esterni non autorizzati	**SI**	Rischio danneggiamento o perdita dati. Gravità **Bassa**
Intercettazioni di informazioni in rete	**SI**	Rischio danneggiamento, sottrazione o perdita dati. Gravità **Bassa**
Eventi relativi al contesto		
Accessi non autorizzati a locali ad accesso ristretto	**SI**	Rischio danneggiamento, sottrazione o perdita dati informatici e cartacei. Gravità **Bassa**
Sottrazione di strumenti contenti dati	**SI**	Rischio danneggiamento, sottrazione o perdita dati informatici e cartacei. Gravità **Bassa**
Eventi distruttivi, naturali o artificiali, nonché dolosi, accidentali o dovuti a incuria	**SI**	Rischio danneggiamento, sottrazione o perdita dati informatici e cartacei. Gravità **Bassa**
Guasto ai sistemi complementari/ausiliari	**SI**	Rischio danneggiamento, sottrazione o perdita dati informatici e cartacei. Gravità **Bassa**
Errori umani nella gestione della sicurezza fisica	**SI**	Rischio danneggiamento o perdita dati informatici e cartacei. Gravità **Bassa**

AIAS di Milano ha provveduto ad elaborare e aggiorna un'analisi dei rischi specifica rispetto alle diverse aree di trattamento, alle diverse tipologie di dati trattati e ai diversi rischi; tale attività,

svolta in collaborazione con il DPO, fornisce elementi utili alla pianificazione degli interventi di miglioramento.

Misure di sicurezza adottate
L'accesso fisico alle stanze contenti documenti trattanti dati personali è permesso solo agli incaricati del trattamento.

Gli armadi in cui sono detenuti documenti cartacei inerenti dati personali devono essere dotati di serratura a chiave. Il Responsabile del trattamento si occupa della gestione delle chiavi in oggetto.
Sono state fornite istruzioni organizzative e tecniche ad hoc per la custodia e l'uso di supporti rimovibili contenenti dati sensibili e giudiziari (chiavette, hard disk, cd riscrivibili, ecc.).

AIAS ha attivato un sistema d'autenticazione per ognuno degli incaricati che trattano dati personali. È stato attribuito un codice identificativo (username, user ID) strettamente personale per l'utilizzazione degli strumenti elettronici (di solito personal computer) del sistema informatico dell'Associazione. I codici identificativi sono frequentemente aggiornati, inserendo quelli dei nuovi incaricati e cancellando quelli degli incaricati non più autorizzati. Il sistema di autenticazione prevede l'utilizzo di parole chiave (password) sia a livello di sistema operativo sia a livello di singola applicazione. Il Responsabile del trattamento è Incaricato della gestione delle password.
Viene segnalato agli incaricati che la lunghezza della password da utilizzare non deve essere inferiore ad otto caratteri, salvo limitazioni tecniche nei software in uso. Si sollecita l'Incaricato che riceve una password a modificarla al primo utilizzo. L'Incaricato deve segnalare al Responsabile del trattamento la sua password in uso. Viene segnalato ad ogni Incaricato la necessità di cambiare la password almeno ogni 6 mesi. È prevista una scadenza nella validità di ogni password utilizzata in AIAS. Sono vietate in AIAS credenziali di autenticazione (username e password) condivise fra più persone. Le credenziali di autenticazione non utilizzate da almeno sei mesi vengono disattivate. Le credenziali di autenticazione vengono immediatamente revocate in caso di provvedimenti disciplinari o quando si presentano situazioni che possono compromettere la sicurezza. Sono state consegnate istruzioni scritte agli incaricati in merito alle modalità di gestione e di custodia delle password. In caso di prolungata assenza dell'Incaricato, il Responsabile del trattamento è autorizzato ad rivelare la password in uso per assicurare la disponibilità dei dati e degli strumenti elettronici. La visualizzazione della password sullo schermo dei personal computer è impedita da tutti i software in uso. Il sistema di identificazione ed autenticazione è operativo anche sui computer portatili.

AIAS si è dotata del seguente software:

Nome prodotto antivirus in dotazione	Bitdefender Gravity-zone versione ULTRA
Descrizione prodotto	L'antivirus in oggetto controlla in automatico ogni file scaricato dalla rete o dalla posta elettronica o letto da supporti esterni quali cd-rom e chiavette
Modalità di aggiornamento	L'aggiornamento del prodotto antivirus installato è

	continuo e fatto automaticamente tramite una funzionalità a disposizione nel prodotto stesso.
Incaricato aggiornamento	Incaricati

AIAS si è dotata dei seguenti sistemi operativi:

Nome prodotto in dotazione	Windows 10, Windows 11
Descrizione prodotto	Sistema operativo
Modalità di aggiornamento	L'aggiornamento del prodotto installato è continuo e fatto automaticamente tramite una funzionalità a disposizione nel prodotto stesso.
Incaricato aggiornamento	Incaricati

Nome prodotto in dotazione	Microsoft Office 2016
Descrizione prodotto	Applicazioni per la realizzazione di testi, fogli di calcolo…
Modalità di aggiornamento	L'aggiornamento del prodotto installato è continuo e fatto automaticamente tramite una funzionalità a disposizione nel prodotto stesso.
Incaricato aggiornamento	Incaricati

Nome prodotto in dotazione	Arca Evolution
Descrizione prodotto	Gestione contabilità generale, clienti, fatturazione
Modalità di aggiornamento	L'aggiornamento del prodotto installato è garantito dalla possibilità di richieste di assistenza alla ditta produttrice, sia on-site che da remoto.
Frequenza aggiornamento	Stabilita dal produttore
Incaricato aggiornamento	Responsabili del Servizio-Amministrazione

Nome prodotto in dotazione	Beatrix 2013
Descrizione prodotto	Gestione socio-sanitario
Modalità di aggiornamento	L'aggiornamento del prodotto installato è garantito dalla possibilità di richieste di assistenza alla ditta produttrice, sia on-site che da remoto.
Frequenza aggiornamento	Stabilita dal produttore
Incaricato aggiornamento	Responsabili del Servizio-Amministrazione

Nome prodotto in dotazione	Contass e RC Presenze
Descrizione prodotto	Gestione presenze
Modalità di aggiornamento	L'aggiornamento del prodotto installato è garantito dalla

	possibilità di richieste di assistenza alla ditta produttrice, sia on-site che da remoto.
Frequenza aggiornamento	Stabilita dal produttore
Incaricato aggiornamento	Responsabili del Servizio-Amministrazione

AIAS si è dotata del seguente sistema firewall

Nome prodotto	Watchguard T40/T20
Incaricato alla gestione e all'aggiornamento	Direzione tramite incaricati assistenza software

Al fine di garantire non solo la integrità, ma anche la pronta disponibilità dei dati, AIAS si è dotata di strumenti e procedure di backup. Si è valutata il sistema e la capienza dello strumento scelto più che sufficiente per la mole di dati attualmente gestita dall'Associazione. Tutti i dati personali gestiti con strumenti elettronici in AIAS vengono inclusi nella procedura di backup. La frequenza con cui vengono effettuate le copie di sicurezza è giornaliera.

Il tempo necessario per recuperare i dati delle copie di sicurezza, a fronte di una generica emergenza, viene stimato in poche ore dal verificarsi del possibile accadimento negativo.

Sono impartite agli incaricati istruzioni scritte, finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura degli uffici, nei luoghi contenenti gli archivi contenenti dati sensibili o giudiziari sono identificate e registrate. La Direzione è incaricata della gestione delle autorizzazioni nei luoghi contenenti dati sensibili.

COVID 19 – GREEN PASS

La pandemia da Covid 19 e l'esigenza di implementare misure strumentali e organizzative di sicurezza al fine di prevenire il contagio e contenere la diffusione del virus, hanno determinato un'esigenza di controllo che, fisiologicamente, investe la tematica privacy, trattandosi di dati personali e sensibili (dati sanitari).

Le procedure di triage nelle diverse strutture e servizi, prevedono il controllo della temperatura. Tale controllo, che rivela un dato biometrico, non produce problematiche rilevanti in tema privacy, poiché nessun dato è registrato e conservato.
Le autodichiarazioni, per lavoratori, collaboratori, volontari, fornitori e utenti, sono invece

necessariamente archiviate nel rispetto delle misure di sicurezza previste.

Il controllo del Green Pass, introdotto dal D.L. 127/2021, prevede che il datore di lavoro controlli la presenza e la validità del Green Pass per tutti i lavoratori e i volontari che entrano in struttura; la valutazione dei rischi per la sicurezza ha inoltre determinato per AIAS di Milano anche la necessità di controllare i Green Pass dell'utenza adulta che accede alle strutture e dell'utenza minorenne (over 12) che partecipa ad attività in compresenza e(o di gruppo.
Tale controllo viene effettuato nel rispetto della normativa privacy, utilizzando dispositivi mobili (cellulari aziendali o dispositivi automatici di lettura del QR code) che lavorano in connessione con la banca dati europea e che non forniscono all'addetto al controllo alcun dato personale.
Anche in questo caso nessun dato viene registrato o archiviato.

CODICE DI CONDOTTA

Premessa

I dipendenti, i collaboratori, i soci e i volontari devono ispirarsi ad un principio generale di diligenza e correttezza nell'utilizzo delle risorse informatiche, telematiche e del patrimonio informativo di AIAS Ogni utilizzo del sistema informativo dell'Associazione diverso da finalità strettamente professionali è espressamente vietato.
Di seguito vengono esposte regole minime comportamentali da seguire per evitare e prevenire condotte che anche inconsapevolmente potrebbero comportare rischi alla sicurezza dei dati personali e sensibili trattati, nonché del sistema informativo e all'immagine di AIAS.
AIAS s'impegna a formare gli autorizzati/incaricati in merito ai rischi, alle procedure operative, alla prevenzione dei danni e, più in generale, alle problematiche relative alla sicurezza in materia di trattamento dei dati.
Il regolamento deve essere portato a conoscenza e distribuito a tutti i componenti dell'Associazione.

L'accesso e l'utilizzo dei dati "sensibili" è consentito ai soli incaricati del trattamento, preposti caso per caso alle specifiche fasi delle attività istituzionali dell'ente secondo il principio della pertinenza dei dati di volta in volta trattati.

Utilizzo dell'elaboratore e/o della rete interna
L'accesso all'elaboratore della propria postazione di lavoro, sia esso collegato in rete o "stand alone", è protetto da un sistema di autenticazione.
AIAS ha attivato un sistema d'autenticazione per ognuno degli incaricati che trattano dati personali.
È stato attribuito un codice identificativo (username, user ID) strettamente personale per l'utilizzazione degli strumenti elettronici (di solito personal computer) del sistema informatico di AIAS. La password assegnata non deve essere divulgata e deve essere custodita dall'assegnatario con la massima diligenza. Il sistema di autenticazione prevede l'utilizzo di parole chiave (password) sia a livello di sistema operativo sia a livello di singola applicazione. Il Responsabile del trattamento è Incaricato della gestione delle password.
Viene segnalato agli incaricati che la lunghezza della password da utilizzare non deve essere inferiore ad otto caratteri, salvo limitazioni tecniche nei software in uso. Si sollecita l'Incaricato che riceve una password a modificarla al primo utilizzo. L'Incaricato deve segnalare al Responsabile del trattamento o al custode nominato la sua password in uso. Viene segnalato ad ogni Incaricato la necessità di cambiare la password almeno ogni 6 mesi.
È vietato istallare qualsiasi software anche demo, senza autorizzazione.
Su ogni elaboratore dell'Associazione è stato installato un software antivirus ed un firewall per prevenire eventuali danneggiamenti all'hardware o al software causati dalla presenza o dall'azione di programmi virus informatici. È importante utilizzare questi software antivirus per controllare qualsiasi file di provenienza esterna ad AIAS. È cura di ciascun operatore controllare che sia stato effettuato l'aggiornamento automatico previsto dal sistema o dallo stesso programma
Si ricorda che nonostante la presenza del software antivirus è possibile che riescano ugualmente ad installarsi nei computer virus informatici non identificati o riconoscibili.

Pertanto in caso si evidenzino anomalie di funzionamento del computer è importante darne rapida segnalazione al Responsabile del trattamento.
L'elaboratore, le unità di rete e le aree di condivisione contengono informazioni strettamente professionali e non possono essere utilizzate per scopi diversi. Non bisogna dislocare stampanti e fax in aree accessibili a soggetti non abilitati al trattamento e non presidiate (ad esempio i corridoi degli uffici).

Gestione supporti rimovibili contenenti dati sensibili
Senza specifica autorizzazione è fatto divieto di usare supporti rimovibili contenenti dati sensibili e giudiziari (chiavette, hard disk, cd riscrivibili, ecc.). È altresì vietato trasferire dati personali e sensibili dai computer di AIAS ai PC personali.

Utilizzo servizi vari su internet
I servizi on line devono essere esclusivamente finalizzati al reperimento di informazioni utili all'Associazione.
Ogni altra utilizzazione dell'accesso su internet, non finalizzata al reperimento di informazioni utili all'Associazione, non pertinente all'attività lavorativa o di tipo personale non è consentita. Al fine di non compromettere la sicurezza di AIAS e di prevenire conseguenze legali o di altro genere a carico della stessa, gli utenti dovranno adottare i seguenti comportamenti:
- evitare lo scaricamento di programmi software, anche gratuiti, se non per esigenze strettamente professionali e fatti comunque salvi i casi di esplicita autorizzazione;
- è vietata la partecipazione a Forum non professionali, l'utilizzo di chat, di bacheche elettroniche e, più in generale, qualunque utilizzo di servizi Internet, attuali o futuri, non strettamente inerenti all'attività professionale;

Utilizzo del servizio di posta elettronica
Il servizio di posta elettronica viene fornito per permettere la comunicazione con soggetti terzi interni ed esterni per le finalità dell'Associazione ed in stretta connessione con l'effettiva attività e mansioni del soggetto dipendente o collaboratore che utilizza tale funzionalità.
Non è possibile utilizzare tale servizio per finalità in contrasto con quelle di AIAS, o non pertinenti all'attività lavorativa o personali.
Al fine di non compromettere la sicurezza di AIAS e di prevenire conseguenze legali a carico della stessa bisogna adottare le seguenti norme comportamentali:
- se nonostante i controlli preventivi antispamming e antivirus automatici, si ricevono mail da destinatari sconosciuti contenenti file (in particolare programmi eseguibili o file di word processor e fogli di calcolo contenenti delle macro, file compressi) evitare di aprire tali mail e tali file e procedere alla loro immediata eliminazione. Il comportamento sopradescritto va seguito anche se si ricevono file non concordati da destinatari conosciuti;

- è fatto divieto di utilizzare le caselle di posta elettronica per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail list salvo diversa ed esplicita autorizzazione;
- la casella di posta elettronica assegnata deve essere mantenuta in ordine, cancellando i documenti inutili specialmente se contengono allegati ingombranti come dimensione;

Gestione dei documenti cartacei
La documentazione cartacea contenente dati personali o sensibili deve essere protetta in appositi armadi dotati di chiavi. Le chiavi devono essere conservate a cura del Responsabile dell'ufficio.

Ogni volta che un soggetto autorizzato preleva documenti contenenti dati sensibili da tali archivi è tenuto a lasciarne traccia mediante apposita segnalazione riportante il proprio nome, data e ora del prelevamento in un apposito registro.
Tutti i documenti contenenti dati personali o aziendali che si ritiene debbano essere eliminati devono essere distrutti e non gettati nei cestini.
È vietato il deposito di documenti di qualsiasi genere negli ambienti di transito o pubblici, come per esempio corridoi o sale riunioni.

Comunicazione dei dati
La comunicazione di dati personali e sensibili, comprese relazioni e documenti di servizio e progetto, devono essere comunicati solamente a soggetti della rete e per motivazione di servizio previa precedente autorizzazione. È altresì vietato l'uso di dati personali, indirizzi, indirizzi mail, numeri telefonici per uso personale e non coerente con gli scopi istituzionali dell'Associazione.

Milano, il 02 Ottobre 2023

per il CD il Presidente e Titolare del trattamento
Dott. Nunzio Bonaccorso