INFORMATIVA PIATTAFORME

Con la presente informativa relativa alle piattaforme gestite dalla società Start To Fly si desidera illustrare a tutti gli interessati quali sono le informazioni raccolte e come le stesse vengono processate.

TITOLARE DEL TRATTAMENTO.
START TO FLY S.R.L. con sede legale in Strada Torinia 10 - Serravalle - RSM - COE: SM26888

BASI GIURIDICHE, FINALITÀ E CONSERVAZIONE.
Ogni trattamento deve trovare fondamento in un'idonea base giuridica, tenuto conto delle finalità per le quali i dati personali sono trattati.
La seguente tabella intende rappresentare in maniera chiara e sintetica quali sono le finalità e le basi giuridiche dei trattamenti effettuati nel corso del rapporto in essere con gli Utenti del sito.

Trattamento/Piattaforma	Finalità dell'attività di trattamento	Base Giuridica	Data retention
a) docenti.it	L'interessato inserisce i propri dati. Poi viene supportato nella redazione del CV ed inserito nelle liste "MAD" e e-commerce per corsi di formazione per docenti.	Adempimento di obblighi contrattuali e di legge.	10 anni
b) elencosupplenti.it	E' portale fornito alle scuole per la ricerca dei c.d. "supplenti". Il portale attinge dalle MAD create con Docenti.it	Adempimento di obblighi contrattuali e di legge. In questo caso, Start To Fly agisce come responsabile esterno della scuola in forza di nomina ex art 28 GDPR	10 anni o differente data retention imposta dalla scuola.
c) aggiornamentograduatorie.it	Portale dove il laureato accede, inserisce i dati e verifica dove può posizionarsi al meglio	Adempimento di obblighi contrattuali e di legge.	10 anni
d) uniscuola.it	E- commerce per corsi di formazione per docenti	Adempimento di obblighi contrattuali e di legge.	10 anni
e) IoMiLaureo.it	E- commerce per corsi di formazione	Adempimento di obblighi contrattuali e di legge.	10 anni
f) congiuntivi.it	E- commerce per corsi di formazione	Adempimento di obblighi contrattuali e di legge.	10 anni
g) Raccolta dati sensibili	Al fine di erogare i servizi richiesti, in alcuni casi sarà necessario raccogliere anche dati particolarmente sensibili come, ad esempio, dati sullo stato di salute o dati giudiziari.	Consenso	10 anni
h) Marketing e soft spam	Iscrivendosi alle piattaforme di Start To Fly, l'utente può decidere di ricevere, o meno, comunicazioni di marketing. Si precisa che, ove ne ricorrano i presupposti, l'utente potrebbe essere contattato in forza di legittimo interesse.	Consenso o legittimo interesse del titolare	2 anni
i) Cessione dati dati a terzi	Con il consenso dell'utente, i dati possono essere ceduti a terzi per finalità di marketing	Consenso	2 anni

TIPOLOGIA DATI TRATTATI
I dati richiesti sono quelli necessari per erogare il servizio correttamente. In alcuni casi sarà, ad esempio, necessario inserire tutti i titoli di cui si è in possesso e i servizi prestati nelle scuole, laurea, diploma, master, certificazioni, abilitazioni e contratti lavorativi svolti nel triennio per determinare il proprio punteggio che poi servirà per posizionarsi nelle graduatorie. Vengono poi solitamente richiesti i dati di contatto utilizzati per contatti correlati al servizio ovvero, in presenza di base giuridica, per comunicazioni marketing come sopra.

CONSEGUENZE DEL MANCATO CONFERIMENTO DATI
L'Utente non è in alcun modo obbligato a fornire i dati. Si precisa però che in mancanza di alcune informazioni potrebbe non essere possibile rispondere alle sue richieste. Si evidenzia che, per alcune tipologie di trattamento, come sopra evidenziato, è richiesto il consenso. Il consenso è sempre revocabile senza che ciò infici la legittimità dei trattamenti effettuati in sua vigenza.

2.COOKIE

Le piattaforme di Star To Fly (d'ora in avanti anche solo "le Piattaforme") utilizzano cookie al fine di consentire all'Utente una migliore esperienza di navigazione.

Cosa sono i cookie?
I cookie sono piccoli file di testo che i siti visitati dagli utenti inviano ai loro terminali, ove vengono memorizzati per essere poi ritrasmessi agli stessi siti alla visita successiva. I cookie delle c.d. "terze parti" vengono, invece, impostati da un sito web diverso da quello che l'utente sta visitando. Questo perché su ogni sito possono essere presenti elementi (immagini, mappe, suoni, specifici link a pagine web di altri domini, ecc.) che risiedono su server diversi da quello del sito visitato (fonte: www.garanteprivacy.it).

I cookie e, in buona misura, gli altri strumenti di tracciamento, possono avere caratteristiche diverse sotto il profilo temporale e dunque essere considerati in base alla loro durata (di sessione o permanenti), ovvero dal punto di vista soggettivo (a seconda che il publisher agisca autonomamente o per conto della "terza parte").

E tuttavia la classificazione che risponde alla ratio della disciplina di legge e dunque anche alle esigenze di tutela della persona, è quella che si basa, in definitiva, su due macro categorie:
- i cookie tecnici, utilizzati al solo fine di "effettuare la trasmissione di una comunicazione su una rete di comunicazione elettronica, o nella misura strettamente necessaria al fornitore di un servizio della società dell'informazione esplicitamente richiesto dal contraente o dall'utente a erogare tale servizio";
- i cookie di profilazione, utilizzati per ricondurre a soggetti determinati, identificati o identificabili, specifiche azioni o schemi comportamentali ricorrenti nell'uso delle funzionalità offerte (pattern) al fine del raggruppamento dei diversi profili all'interno di cluster omogenei di diversa ampiezza, in modo che sia possibile inviare messaggi pubblicitari sempre più mirati, cioè in linea con le preferenze manifestate dall'utente nell'ambito della navigazione in rete.

Tipologia del trattamento
Le Piattaforme utilizzano i cookie meglio indicati nella Cookie Management Plattform a cui si rinvia per la gestione degli stessi.

Come disabilitare/cancellare i cookie utilizzando i browser più comuni?
Chrome
1. Avviare Chrome sul device.
2. In alto a destra cliccare l'icona con i tre pallini e poi posizionarsi su "Impostazioni".
3. Nella finestra, in basso, cliccare su "Avanzate".
4. Sotto la voce "Privacy e Sicurezza" cliccare "Impostazione Contenuti".
5. Cliccare "Cookie".
6. In questa sezione si potranno disabilitare tutti o solo alcuni cookie.

Maggiori dettagli su: https://support.google.com/accounts/answer/61416?hl=en

Mozilla Firefox
1. Avviare Firefox sul tuo device.
2. Cliccare il tasto "Menù" (rappresentato da un tasto con tre righe parallele, posizionato in alto a destra), e poi selezionare "Opzioni".
3. Selezionare il pannello "Privacy e Sicurezza" e poi andare al paragrafo "Cookie e dati dei siti web".
4. In questa sezione si potrà decidere quali cookie ricevere e per quanto tempo conservarli sul device.

Maggiori dettagli su: https://support.mozilla.org/en-US/kb/enable-and-disable-cookies-website-preferences

In ogni caso ricordiamo che esistono anche altre opzioni per navigare senza cookie:

Blocca i cookie di terze parti
I cookie di terze parti non sono generalmente indispensabili per navigare, quindi possono essere rifiutati per default, attraverso apposite funzioni del browser.

Attiva l´opzione Do Not Track
L'opzione Do Not Track è presente nella maggior parte dei browser di ultima generazione. I siti web progettati in modo da rispettare questa opzione, quando viene attivata, dovrebbero automaticamente smettere di raccogliere alcuni tuoi dati di navigazione. Come detto, tuttavia, non tutti i siti web sono impostati in modo da rispettare questa opzione (discrezionale).

Attiva la modalità di "navigazione anonima"
Mediante questa funzione è possibile navigare quasi senza lasciare traccia nel browser dei dati di navigazione. I siti non si ricorderanno dell'utente, le pagine non saranno memorizzate nella cronologia e i nuovi cookie saranno cancellati.

La funzione navigazione anonima non garantisce comunque l'anonimato su Internet, perché serve solo a non mantenere i dati di navigazione nel browser, mentre invece i dati di navigazione continueranno a restare disponibili ai gestori dei siti web e ai provider di connettività.

Elimina direttamente i cookie
Ci sono apposite funzioni per farlo in tutti i browser. Si ricorda però che ad ogni collegamento ad Internet vengono scaricati nuovi cookie, per cui l'operazione di cancellazione andrebbe eseguita periodicamente. Volendo, alcuni browser offrono dei sistemi automatizzati per la cancellazione periodica dei cookie.

A CHI COMUNICHIAMO I DATI
Esclusivamente per le finalità sopra indicate, i dati dell'Utente potrebbero essere trasmessi a:

PERSONE AUTORIZZATE AL TRATTAMENTO: sono figure interne, nello specifico soci, dipendenti e collaboratori del Titolare del Trattamento, che raccolgono o elaborano i dati in ragione delle rispettive mansioni e secondo i profili attribuiti.
RESPONSABILI DEL TRATTAMENTO: sono collaboratori terzi che trattano dati per conto del Titolare del Trattamento, mediante la stipula di un apposito accordo di nomina a Responsabile del Trattamento, a mezzo del quale sono definite le operazioni delegate al terzo, nonché le misure di sicurezza che questi deve adottare al fine di tutelare al meglio le informazioni che ottiene dallo stesso Titolare. In particolare, potrebbero trattare i Suoi dati:

- Servizio di hosting per la e-mail, hosting del sito, servizio per fatture in cloud e gestionale in cloud.

DESTINATARI: sono coloro che ricevono comunicazioni di dati personali da parte del Titolare, ma che, a seguito di tale comunicazione, agiscono in veste di autonomi Titolari. Fra questi:

- . Pubbliche amministrazioni, Enti ed altre Autorità, nei casi espressamente previsti dalla legge.

La sede della società è presso la Repubblica di San Marino, pertanto l'invio di dati avviene in forza di Clausole Contrattuali Standard. In ogni altro caso i dati non verranno trasferiti in paesi esterni allo spazio UE in mancanza di un consenso esplicito ovvero in mancanza delle garanzie a tal fine previste dal GDPR (giudizi di adeguatezza, sottoscrizione di clausole standard…).
La lista dei terzi nominati quali Responsabili del Trattamento è a disposizione della Clientela e dei Fornitori presso la sede, e potrà essere esibita agli Interessati previa apposita richiesta.

DIRITTI DELL'INTERESSATO

Avrà sempre il diritto di ottenere dal Titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che La riguardano e, in tal caso, di ottenere l'accesso ai dati personali e alle informazioni indicate nell'art. 15 GDPR.
Inoltre, Le è riconosciuto il diritto di ottenere la rettifica, la cancellazione e la limitazione al trattamento dei Suoi dati personali in possesso del Titolare.
Infine, Le è riconosciuta la possibilità di proporre reclamo all'autorità di controllo dello Stato Membro in cui risiede/lavora oppure del luogo ove si è verificata la presunta violazione.

DATA PROTECTION AGREEMENT

Il CLIENTE, nel caso in cui, in forza dei servizi concordati nel contratto principale, deleghi al FORNITORE una porzione del trattamento dei dati, nomina quest'ultimo quale responsabile del trattamento, autorizzandolo al trattamento dei relativi dati personali in quanto necessario per l'erogazione dei servizi informatici stessi, nel rispetto dei termini contrattuali di fornitura e secondo quanto stabilito nel presente accordo.

In relazione alla nomina si concorda che:
(a) Le finalità del trattamento dei dati personali trasmessi dal CLIENTE sono esclusivamente quelle di erogare i servizi di cui al precedente comma;
(b) Nell'ambito dei trattamenti consentiti al responsabile del trattamento di cui alla lettera precedente, è compresa anche l'attività di assistenza e consulenza tecnica, l'aggiornamento e la manutenzione dei sistemi informatici utilizzati dal CLIENTE, se del caso anche in modalità "on premise" o da remoto, e possono consistere in tutte le relative operazioni di supporto e quindi a titolo esemplificativo:

i. attività di archiviazione e di concessione accesso ai dati;
ii. attività di migrazione dati finalizzata all'installazione ed al collaudo di software o servizi informatici;
iii. servizi di assistenza e aggiornamento che comportano (ancorché occasionalmente) l'accesso remoto ai dati del CLIENTE;
iv. analisi di dati (DB, videate, esportazioni di dati, ecc.) del CLIENTE per verificare problematiche di carattere tecnico e svolgere attività di manutenzione o supporto tecnico;

(c) Il responsabile del trattamento potrà effettuare i trattamenti in modalità automatizzata sempre in quanto necessario per le finalità innanzi indicate;
(d) Il CLIENTE decide la tipologia di dati personali oggetto del trattamento tramite i servizi informatici forniti dal responsabile del trattamento, i quali possono essere dati personali comuni, di categoria particolare o relativi a condanne o reati;
(e) La categoria di interessati si riferisce a persone fisiche come soggetti presenti nelle MAD, operatori della scuola e utenti;
(f) La durata del trattamento è limitata alla durata del servizio come descritto nelle condizioni generali di fornitura ed al termine i dati personali saranno cancellati secondo quanto contrattualmente stabilito salvo intervento di ulteriore base giuridica;
(g) Il responsabile garantisce che le persone autorizzate al trattamento dei dati personali si sono impegnate alla riservatezza;
(h) Il CLIENTE dichiara e garantisce di avere tutti i poteri necessari per effettuare la nomina del responsabile in relazione ai dati personali che quest'ultimo tratterà per suo conto, nel rispetto della normativa sulla privacy;
(i) Il CLIENTE dichiara e garantisce di aver raccolto i dati in modo legittimo, adempiendo ad ogni formalità prevista dalla normativa italiana ed europea in materia di trattamento dei dati.

Posizione del CLIENTE rispetto ai dati personali oggetto del trattamento
Le parti convengono di considerare il CLIENTE di regola quale titolare del trattamento in relazione ai dati personali oggetto del presente accordo, salvo quanto di seguito indicato.
Nel caso in cui il CLIENTE svolga le operazioni di trattamento per conto di un titolare o un responsabile del trattamento o un sub-responsabile del trattamento, il CLIENTE garantisce che il presente accordo è conforme alle istruzioni ricevute ed ai poteri conferiti, avendo verificato la regolarità della sua posizione prima di sottoscrivere le condizioni generali di fornitura e il presente accordo.
Nel caso previsto dai commi precedenti, il FORNITORE assumerà il ruolo di responsabile del trattamento o sub-responsabile a seconda del ruolo rivestito dal CLIENTE.
In relazione a quanto sopra, il FORNITORE potrà chiedere in qualunque momento la documentazione idonea ad attestare il ruolo privacy del CLIENTE.
Se nel corso del contratto di fornitura, il ruolo del CLIENTE cambia, questi è tenuto a comunicarlo al responsabile del trattamento, con le modalità ivi previste.
Il FORNITORE compilerà il registro del responsabile del trattamento ex art. 30 co. 2 GDPR, indicando il ruolo del CLIENTE, rispetto ai dati personali oggetto del contratto di fornitura, secondo quanto da quest'ultimo dichiarato come innanzi indicato o in mancanza quale titolare del trattamento.
art. 10 Istruzioni del CLIENTE e limiti

Nell'ambito dell'esecuzione del presente accordo, il FORNITORE, quale responsabile del trattamento si adeguerà alle istruzioni del CLIENTE, in relazione ai dati personali oggetto di trattamento, salvo che le operazioni richieste con le istruzioni non siano previste dal presente accordo o comportino variazioni di risorse informatiche e organizzative non comprese nel contratto di fornitura dei servizi.
In quest'ultima ipotesi, il FORNITORE valuterà la fattibilità delle istruzioni e, se fattibile, concorderà con il CLIENTE le suddette variazioni e costi relativi. In mancanza di accordo, le istruzioni non saranno attuate, valendo quanto disciplinato dal presente accordo.
Resta inteso che le istruzioni del CLIENTE anche rientranti nel presente accordo e comunque i trattamenti svolti quale responsabile del trattamento, saranno eseguiti sempreché non comportino, a giudizio del FORNITORE, una violazione della normativa sulla privacy o di un ordine imposto da una pubblica autorità.
In quest'ultimo caso il FORNITORE invierà senza ritardo motivazione scritta al CLIENTE, fatto salvo i divieti previsti dalla legge.

Nomina di altri sub-responsabili da parte di FORNITORE
Il CLIENTE autorizza in via generale il FORNITORE, quale responsabile del trattamento, a nominare sub-responsabili del trattamento per l'esplicazione di parte dei propri compiti purché nel rispetto del contratto di fornitura e del presente accordo.
L'autorizzazione suddetta comporta il potere di aggiungere nuovi sub-responsabili o sostituirli, e modificare i relativi accordi contrattuali.
L'autorizzazione generale conferita è così disciplinata:
(a) Il soggetto nominato dovrà presentare adeguate garanzie di adeguatezza sia in relazione alla sicurezza dei trattamenti e sia in relazione alla tutela dei diritti e libertà degli interessati e comunque rispettoso degli standard di mercato di settore;
(b) I trattamenti dei dati personali svolti dal sub- responsabile saranno limitati solo a quanto necessario per la fornitura dei servizi forniti e in quanto rilevanti e utili per l'esplicazione di una parte dei servizi oggetto del contratto di fornitura del FORNITORE;
(c) La nomina del sub-responsabile sarà effettuata per iscritto, imponendo obblighi di tutela non inferiore a quelli previsti dal presente accordo e dall'art. 28 GDPR;
(d) Il CLIENTE sarà avvisato per iscritto della nomina entro un termine di 180 giorni, potrà opporsi per iscritto entro 30 giorni. Nel caso di opposizione del CLIENTE, il FORNITORE potrà recedere dal contratto di fornitura in essere con il CLIENTE, con preavviso di 30 giorni;
(e) L'elenco dei sub-responsabili nominati dal FORNITORE è messo a disposizione del CLIENTE su sua richiesta;
(f) Le parti concordano fin d'ora per la nomina, quali sub-responsabili, dei fornitori di servizi informatici, anche tramite piattaforme CLOUD, di cui si avvale il FORNITORE, indicati nell'allegato A) alle condizioni generali di fornitura e per le attività ivi indicate. Il CLIENTE dichiara di aver preventivamente verificato la loro affidabilità e l'idoneità dei DPA in relazione alla propria attività.

Vincoli al trasferimento dei dati personali fuori dallo Spazio Economico Europeo (SEE)
Sempre nel rispetto della normativa privacy, il responsabile potrà trasferire esclusivamente per particolari esigenze tecniche, i dati personali del CLIENTE, se possibile tecnicamente tramite sistemi di cifratura secondo standard tecnici riconosciuti a livello internazionale, anche fuori dallo Spazio Economico Europeo (SEE) o da un paese che non goda di una decisione di adeguatezza da parte della Commissione Europea ai sensi dell'art. 45 del GDPR, esclusivamente rispettando una delle seguenti condizioni:
(a) vengano stipulate le clausole contrattuali tipo previste nella Decisione della Commissione Europea 2010/87/UE, del 5 febbraio 2010 e successive modifiche ed integrazioni, con il sub-responsabile del trattamento nominato dal FORNITORE, il quale è autorizzato fin d'ora dal CLIENTE a sottoscriverle;
(b) oppure, se il sub-responsabile del trattamento sia parte di un gruppo societario in relazione a trasferimenti infragruppo, quest'ultimo abbia ottenuto l'approvazione delle BCR (norme vincolanti d'impresa).
Il responsabile del trattamento fornisce al CLIENTE le informazioni e la documentazione idonea in relazione a quanto sopra previsto.
Resta salvo un diverso accordo tra le parti.

Misure di sicurezza adeguate del responsabile del trattamento
Il FORNITORE, quale responsabile del trattamento, si impegna nell'ambito dei trattamenti previsti dal presente accordo ad adottare le misure tecniche ed organizzative adeguate, secondo standard tecnici di mercato, al fine di consentire la tutela della liceità dei trattamenti dei dati personali, la loro riservatezza, integrità, disponibilità e la resilienza dei servizi forniti.
Una sintesi delle misure di protezione adottate sono contenute nella Sezione III A) del presente accordo.
Qualora il CLIENTE richieda di adottare misure tecniche ed organizzative ulteriori, il FORNITORE si riserva di verificare la fattibilità della richiesta e di concordare se del caso, le modalità ed i costi relativi.

Verifiche e controlli
Il CLIENTE ha la facoltà di effettuare, a proprie spese, degli audit di terze parti, anche presso la sede del FORNITORE (concordando previamente una data utile), al fine di verificare gli adempimenti al presente accordo, tramite proprio personale specializzato o professionisti di provata esperienza, in ogni caso vincolati per iscritto ad obblighi di riservatezza. Il FORNITORE potrà opporsi alla nomina di professionisti che siano in conflitto di interesse, non sufficientemente qualificati o non indipendenti e in questo caso il CLIENTE dovrà proporre un diverso nominativo o svolgere direttamente l'audit. La relazione dell'audit sarà messa a disposizione del responsabile del procedimento gratuitamente.
Le modalità di svolgimento dell'audit di cui al punto precedente saranno concordate dalle parti, e il FORNITORE comunicherà il costo orario del proprio personale incaricato di assistervi, comunque non inferiore alla tariffa oraria per l'assistenza tecnica.
Le attività di verifica che interessino eventuali sub-responsabili nominati dal FORNITORE saranno svolte secondo le modalità concordate con questi ultimi, nel rispetto delle loro politiche di conformità alla privacy.

Misure di sicurezza del CLIENTE nel caso di servizi CLOUD
Il CLIENTE è consapevole che la fruizione e la sicurezza dei servizi CLOUD forniti dal FORNITORE richiede una idonea configurazione, che viene decisa in autonomia dal CLIENTE secondo le condizioni generali di fornitura.
Il CLIENTE si impegna a configurare, per quanto di sua competenza, i servizi suddetti in modo da garantire un adeguato livello di protezione in relazione al proprio ambito di trattamento dei dati personali nel rispetto della normativa sulla privacy.
In ogni caso, il CLIENTE terrà prontamente informato il FORNITORE nel caso sospetti o constati violazioni di sicurezza dei servizi acquistati, fornendo idonea documentazione al riguardo.
E' fatto salvo quanto previsto dalle condizioni generali di fornitura nel caso il CLIENTE abbia richiesto i servizi MSP ivi previsti.

Violazioni di dati personali (Data Breach)
Nel caso in cui il FORNITORE venisse a conoscenza di un evento che stia dando luogo o possa aver dato luogo ad una violazione dei dati personali di cui al presente accordo, sarà tenuto ad avvisare il CLIENTE senza ritardo.

In ogni caso il FORNITORE invierà al CLIENTE, senza ritardo e per quanto ragionevolmente possibile, una relazione scritta che descriva i possibili danni cagionati e le cause se conosciute, le misure di protezione adottate per evitare o mitigare i potenziali rischi e suggerendo al CLIENTE le misure opportune a tutela dei dati personali trattati. Quest'ultimo verrà comunque tenuto sempre costantemente aggiornato.
Resta inteso che la comunicazione di cui sopra non costituisce riconoscimento di un inadempimento o responsabilità in capo al responsabile del trattamento, in relazione alla violazione ivi riportata.
Si ricorda che nel rispetto dell'art. 33 e 34 del GDPR, spetti al CLIENTE gestire gli adempimenti relativi alle comunicazioni ivi previste all'Autorità Garante ed agli interessati, sotto la sua esclusiva responsabilità.

Richieste di interessati al responsabile del trattamento e obblighi delle parti
Nel caso in cui il responsabile del trattamento riceva richieste per l'esercizio di diritti da parte di interessati in relazione a dati personali che tratta per conto del CLIENTE in base al presente accordo, sarà tenuto ad inviarle senza ritardo al CLIENTE, il quale si occuperà di gestire le suddette richieste, direttamente o anche tramite il titolare del trattamento se diverso dal CLIENTE stesso.
Il responsabile del trattamento assisterà il CLIENTE fornendogli tutte le informazioni in relazione ai servizi gestiti dal FORNITORE sulla base di quanto previsto dal presente accordo ed inviterà l'interessato a rivolgersi al CLIENTE al fine di esercitare i propri diritti, evidenziando la propria posizione di responsabile del trattamento.
Il CLIENTE si assume quindi ogni responsabilità circa la gestione dei diritti degli interessati, salvo quanto indicato nei due commi precedenti relativamente al responsabile del trattamento.

Richieste di interessati rivolte al CLIENTE per dati personali trattati per suo conto dal responsabile del trattamento
Nel caso in cui il CLIENTE debba soddisfare richieste relative ad interessati per l'esercizio dei loro diritti in relazione a dati personali oggetto del presente accordo, il responsabile del trattamento fornirà le informazioni richieste dal CLIENTE e darà seguito alle istruzioni da quest'ultimo impartite per quanto inerenti al presente accordo, in relazione ai servizi acquistati dal CLIENTE.
In ogni caso il CLIENTE tratterà direttamente la suddetta richiesta, limitandosi il responsabile del trattamento ad adempiere a quanto sopra.

Portabilità dei dati personali
Nel caso in cui sia necessario da parte del CLIENTE soddisfare richieste di portabilità dei dati personali, il responsabile del trattamento fornirà, esclusivamente in relazione ai servizi acquistati dal CLIENTE, solo le informazioni utili per estrarli in formato conforme alla normativa sulla privacy e sempreché ciò sia ragionevolmente possibile.
Nel caso in cui il CLIENTE richieda invece l'assistenza tecnica necessaria per effettuare la suddetta estrazione, il FORNITORE ne valuterà la fattibilità tecnica e concorderà con il primo, se del caso, le modalità relative e i costi a carico del CLIENTE.

Amministratore di sistema
Come previsto dal provvedimento del Garante della Privacy del 27 novembre 2008 e dalla modifica intervenuta in data 26 giugno 2009, i titolari del trattamento sono tenuti a nominare i soggetti esterni -incaricati della manutenzione e gestione di sistemi informatici- quali responsabili del trattamento, con obbligo in capo questi ultimi di individuare al loro interno il nome e cognome degli effettivi amministratori di sistema che opereranno sui sistemi informatici del CLIENTE.
In tal senso, nei casi previsti dal succitato provvedimento dell'Autorità Garante, Start To Fly assume il particolare ruolo di responsabile esterno del trattamento con funzioni di amministratore di sistema.
Le persone fisiche che operano sotto l'autorità diretta del responsabile e che prestano la loro attività presso il CLIENTE, finalizzata all'assistenza e/o manutenzione dei sistemi informativi, servizi informatici e reti, acquisiscono la qualifica di amministratore di sistema e sono tenute al rispetto delle disposizioni previste dal Provv. n. 300/2008 ss. mod. dell'Autorità Garante per la protezione dei dati personali.
Il responsabile terrà elenchi aggiornati dei soggetti adibiti al ruolo di amministratori di sistema che comunicherà periodicamente (almeno una volta all'anno) al titolare.
Il FORNITORE garantisce che l'operato degli amministratori di sistema sarà oggetto, con cadenza almeno annuale, di un'attività di verifica da parte del responsabile in modo da controllare la rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti. Il report di tale attività verrà inviato anche al CLIENTE su espressa richiesta.
Infine il FORNITORE, ove possibile, si impegna ad adottare sistemi idonei alla registrazione degli accessi logici (dandone visibilità ed accesso al CLIENTE su richiesta) da parte degli amministratori di sistema. Le registrazioni (access log) avranno caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni comprenderanno i riferimenti temporali e la descrizione dell'evento che le ha generate e saranno conservate per un congruo periodo, non inferiore a sei mesi.

PRINCIPALI MISURE DI PROTEZIONE

A) MISURE ORGANIZZATIVE
1. Adozione di una politica sulla gestione della sicurezza delle informazioni e di una politica per la tutela dei dati personali in conformità alla normativa privacy, basate sull'analisi del rischio, al fine di garantire la riservatezza, disponibilità ed integrità dei dati personali a tutela dei diritti e libertà degli interessati;
2. Procedure di accesso alle strutture fisiche, debitamente protette, solo a soggetti autorizzati previo idoneo riconoscimento;
3. Policy e Disciplinari utenti: Vengono applicate dettagliate policy e disciplinari, ai quali tutta l'utenza con accesso ai servizi informatici deve conformarsi a garanzia della sicurezza dei sistemi;
4. Autorizzazione accessi logici – Tutti i sistemi informatici sono accessibili solo con profili di accesso per quanto necessario alla mansione svolta. I profili di autorizzazione sono individuati e configurati preventivamente all'accesso;
5. Presente una procedura di gestione degli incidenti collegata a strumenti tecnici di monitoraggio dei sistemi cui è proposto personale specializzato, con individuazione, in caso di incidente, degli interventi da predisporre secondo un ordine logicamente determinato, con lo scopo di garantire il ripristino dei servizi nel più breve tempo possibile, nonché verificarne le conseguenze, redigere un report, dal cui esito dipendono ulteriori misure di protezione, ferma in ogni caso la verifica dell'adeguatezza dei sistemi di protezione predisposti;
6. Procedura di gestione dell'assistenza – Gli interventi di assistenza vengono gestiti mediante una procedura che verifichi l'autenticità della richiesta ed eroghi il supporto contenendo al minimo il trattamento dati personali, tramite personale debitamente formato e strumenti tecnici rispettosi degli standard di sicurezza. Anche tramite un servizio di ticket system messo a disposizione del CLIENTE, sarà sempre possibile sapere il dettaglio dell'intervento, durata, data e l'operatore (tramite un codice univoco a lui assegnato), nonché verificare, da parte del responsabile del trattamento, l'autenticità della richiesta di supporto;
7. Ogni dipendente può trattare solo le informazioni per i quali è stato autorizzato in relazione alle mansioni svolte nonché debitamente formato, mediante aggiornamenti periodici, per trattare i dati con la massima riservatezza e sicurezza, nel rispetto della normativa privacy;
8. Regolamento interno per i dipendenti, circa l'utilizzo degli strumenti informatici e sui potenziali controlli del datore di lavoro;

9. Procedure di protezione contro attacchi tramite social engineering con collegata specifica formazione del personale;
10. Procedure per la scelta dei fornitori adeguati incentrate sulla verifica di qualità, sicurezza e conformità alla normativa vigente dei beni o servizi offerti;
11. Data Breach – Esiste una procedura per la gestione degli incidenti che possa incidere sui dati personali, basata sulla distribuzione dei ruoli secondo competenza, verifica del potenziale pregiudizio (presunto o accertato), gestione delle contromisure nonché le modalità di condivisione con il CLIENTE delle informazioni relative alle violazioni di dati personali e per l'adozione degli adempimenti connessi previsti dalla normativa privacy;
12. Aggiornamento delle misure organizzative che saranno verificate ogni sei mesi;

B) MISURE TECNICHE

1. Credenziali di autenticazione – L'accesso ai sistemi si basa esclusivamente su credenziali di autenticazione univoche, basate su un PIN o chiave di accesso riservate e con misure di sicurezza conformi a standard internazionali;
2. Gestione password di accesso secondo best practice, basate sulla lunghezza, complessità, scadenza, robustezza affidate a soggetti debitamente istruiti circa il suo utilizzo e conservazione;
3. Amministratori di Sistema – Per gli utenti con ruolo di Amministratori di Sistema, le cui mansioni sono attribuite con atti di nomina specifici ed in forma scritta, è implementato un sistema di log management non alterabile debitamente configurato per tracciare le attività svolte e consentire il monitoraggio successivo per la verifica della regolarità delle operazioni. E' attiva poi una procedura per la verifica dell'operato degli amministratori di sistema nell'ambito del piano di sicurezza delle informazioni elaborato internamente e per la conformità rispetto alla normativa sulla privacy ed anche al fine del miglioramento delle misure di protezione;
4. Utilizzo di sistemi di cifratura basati su algoritmi e protocolli informatici conformi a standard internazionali;
5. Adozione di sistemi Firewall quali componenti di difesa perimetrale delle reti informatiche ed a tutela delle linee di comunicazione;
6. Antivirus e Malware aggiornati con cadenza periodica contro il rischio di intrusione e dell'azione illecita di programmi;
7. Sistemi di logging al fine del monitoraggio dei sistemi, conservazione degli eventi accaduti ed identificazione degli accessi;
8. Sistemi di backup & restore, con relativa procedura di gestione;
9. Business continuity per la resilienza dei sistemi in caso di incidente;
10. Aggiornamento constante dei sistemi informatici, delle misure tecniche, al variare della tecnologia e con costante verifica secondo tempistiche prestabilite nonché verifica costante, presso fonti affidabili, dei problemi di sicurezza dei prodotti e servizi informatici in uso per l'update relativo.