

DPA – Data Processing Agreement

Accordo sul Trattamento dei Dati Personali

(ex. art.28 Regolamento UE 2016/679)

PREMESSA

Axios Italia Service S.r.l. SU con sede in Via E. Filiberto 190 – 00185 Roma, P.IVA 06331261005 (di seguito AXIOS), da oltre 30 anni, sviluppa software per la gestione delle Segreterie Scolastiche nelle Scuole sia nell'utilizzo in locale (client/server) che su web.

Obiettivo principale dell'azienda, oltre quello di rendere agevole il lavoro quotidiano dei nostri clienti, è quello di garantire la sicurezza degli applicativi adeguandoli alle normative che si sono susseguite negli anni. Per questo motivo, AXIOS si è impegnata e ha ottenuto le certificazioni ISO 9001:2015, ISO 27001:2013, ISO 27018:2014 e ISO 27017:2015 per i seguenti campi applicativi: "Progettazione, sviluppo, manutenzione e assistenza di software gestionale e servizi SaaS connessi" ed inoltre, da aprile 2019, la qualifica AgID secondo la circolare n.3 del 9 aprile 2018 per gli applicativi SaaS.

AXIOS, attraverso il presente Accordo, intende informare il TITOLARE in merito alle modalità di trattamento dei dati e alle misure di sicurezza adottate nel rispetto di quanto previsto dal Regolamento UE 2016/679 (di seguito RGPD - Regolamento Generale per la Protezione dei Dati) e delle altre normative vigenti in materia di protezione dei dati personali.

DEFINIZIONI

Ai fini del presente accordo i termini e le espressioni che seguono dovranno intendersi come di seguito indicato:

- ✓ Sono da intendersi valide tutte le definizioni così come indicate nell'art.4 dell'RGPD;
- ✓ Si tiene conto anche delle definizioni indicate nell'ALLEGATO "A" (CONDIZIONI DI LICENZA D'USO SOFTWARE AXIOS E RELATIVA ASSISTENZA);
- ✓ Per semplicità espositiva, peraltro adottata frequentemente nella dottrina, si definisce "responsabile del trattamento" colui che tratta i dati per conto di un titolare del trattamento mentre si definisce "sub-responsabile" colui che tratta i dati per conto di un responsabile del trattamento.

OGGETTO

Considerato che tra la AXIOS (di seguito RESPONSABILE) e l'Istituto scolastico (di seguito TITOLARE) rappresentato legalmente dal Dirigente Scolastico (pro tempore) è stipulato, ed è in corso di validità, un Contratto per la fornitura di software gestionale per la segreteria scolastica (programmi client/server per sistemi Microsoft Windows) e servizi gestionali in SaaS (su piattaforma web) per l'attività amministrativa e didattica riguardanti l'elaborazione in locale e on line dei dati di cui l'Istituto scolastico è TITOLARE (inclusi relativi servizi di assistenza tecnica e manutenzione), ai sensi dell'art.28 dell'RGPD, sulla base del presente Accordo AXIOS agirà quale RESPONSABILE del trattamento in relazione alle attività di trattamento dei dati personali conferiti dal TITOLARE ai soli fini dell'esecuzione del Contratto.

Il trattamento potrà essere svolto sia in forma automatizzata sia in forma non automatizzata.

Il presente Accordo intende disciplinare i diritti e gli obblighi spettanti al RESPONSABILE e al TITOLARE relativamente al rispetto della normativa in materia di protezione dei dati personali (Regolamento UE 2016/679, D.lgs. 196/03 come modificato dal D.lgs. 101/18, e altre normative vigenti in materia di protezione dei dati personali).

OBBLIGHI DEL TITOLARE

Il TITOLARE garantisce che:

- ✓ i Dati Personali conferiti al RESPONSABILE sono nella sua piena disponibilità nel rispetto di quanto previsto dall'RGPD e dalla legislazione in materia di protezione delle persone fisiche a riguardo del trattamento dei dati;
- ✓ i Dati personali conferiti al RESPONSABILE sono esatti e aggiornati.

DATI PERSONALI TRATTATI E CATEGORIE DI INTERESSATI

Le categorie di dati personali trattati sono:

- ✓ Credenziali di accesso e log relativi agli accessi e all'utilizzo delle applicazioni;
- ✓ dati identificativi e anagrafici in generale (es. nome, cognome, e-mail, numeri di telefono, indirizzo IP, etc.);
- ✓ dati di fatturazione, contabilità e pagamenti;
- ✓ dati ex. art.9 (categorie particolari di dati personali; es. dati relativi allo stato di salute);
- ✓ dati ex. art.10 (dati personali relativi a condanne penali o a reati o a connesse misure di sicurezza ...);
- ✓ dati statistici o altri dati di navigazione in rete.

I dati personali raccolti e trattati si riferiscono alle seguenti tipologie di interessati:

- ✓ Alunni
- ✓ Dipendenti
- ✓ Genitori
- ✓ Familiari
- ✓ Tutori
- ✓ Fornitori (Aziende, Consulenti, etc.)

COMUNICAZIONE VIOLAZIONI DELLA SICUREZZA

Il TITOLARE comunica senza ingiustificato ritardo al RESPONSABILE, attraverso i canali di comunicazione messi a disposizione da AXIOS (mail, PEC, telefono) eventuali o potenziali violazioni della sicurezza che coinvolgano o meno dati personali.

OBBLIGHI DEL RESPONSABILE

Il RESPONSABILE è tenuto a rispettare tutti i requisiti di legge previsti dagli artt. 28-33 RGPD. A tal fine, il RESPONSABILE garantisce quanto segue:

NOMINA DI UN RESPONSABILE PER LA PROTEZIONE DEI DATI PERSONALI (RPD/DPO)

AXIOS ha nominato un Responsabile per la protezione dei dati. L'attuale DPO è il Sig. De Vita Vincenzo, indirizzo mail: dpo@axiositalia.com . Il RESPONSABILE segnalerà al TITOLARE senza indebito ritardo ogni cambio di DPO.

RISERVATEZZA

Le attività di trattamento regolate da questo Accordo saranno svolte solo da dipendenti, collaboratori o

incaricati previamente istruiti dal RESPONSABILE sul corretto trattamento di dati personali e contrattualmente soggetti ad obbligo di riservatezza ai sensi degli artt. 28 par. 3 (b) e 32 RGPD. Il RESPONSABILE, così come chiunque agisca sotto la sua autorità ed ha abbia accesso a dati personali, non tratterà dati personali se non istruito in tal senso dal TITOLARE, anche a mezzo del presente Accordo, salvo che per espressa previsione di legge (art. 29 RGPD).

MISURE TECNICHE ED ORGANIZZATIVE

Il RESPONSABILE garantisce la sicurezza del trattamento ai sensi degli artt. 28 par. 3 punto c) e 32 RGPD, in particolare ai sensi dell'art. 5 par. 1 e par. 2 RGPD. Tali misure devono garantire la sicurezza dei dati ed un livello di protezione adeguato al rischio per la confidenzialità, integrità, disponibilità e resilienza dei sistemi. Ai sensi dell'art. 32 par. 1 RGPD, nel valutare il livello di adeguatezza delle misure di sicurezza deve tenersi conto dello stato dell'arte, i costi di realizzazione, la natura, l'oggetto e gli scopi del trattamento, così come la probabilità di una violazione di dati personali e la gravità dei rischi da essa potenzialmente derivanti per i diritti e le libertà delle persone fisiche.

Il RESPONSABILE controlla periodicamente i processi interni e le misure tecniche e organizzative per assicurare che il trattamento nella sua area di competenza sia conforme ai requisiti della normativa sulla protezione dei dati personali e dei diritti degli interessati, ai sensi di quanto specificato dall'art. 32 RGPD. Il RESPONSABILE garantisce al TITOLARE la verificabilità delle misure tecniche e organizzative nell'ambito dei suoi poteri di controllo.

ASSISTENZA AL TITOLARE

Il RESPONSABILE assiste il TITOLARE nell'adempimento degli obblighi relativi alla sicurezza dei dati personali, nella segnalazione di violazioni dei dati, nelle valutazioni d'impatto sulla protezione dei dati e nelle consultazioni preventive di cui agli articoli da 32 a 36 RGPD, tra l'altro garantendo adeguati standard di protezione mediante misure tecniche e organizzative, tenendo conto della natura, delle circostanze e delle finalità del trattamento, della probabilità di violazioni dei dati e della gravità del rischio per le persone fisiche che ne può derivare garantendo l'immediata individuazione delle violazioni e assistendo il TITOLARE nell'evadere le richieste degli interessati di esercizio dei loro diritti.

VIOLAZIONI DELLA SICUREZZA

Ai sensi dell'art. 33 par.2, in caso di violazione dei dati personali, "il RESPONSABILE del trattamento informa il TITOLARE del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione", inviando una comunicazione con il seguente contenuto:

- ✓ la data e l'ora in cui si è verificata la violazione;
- ✓ una descrizione del tipo di violazione e di come è stata identificata;
- ✓ se possibile categorie dei dati personali, numero e tipo di interessati;
- ✓ misure di mitigazione adottate;
- ✓ probabili conseguenze della violazione;
- ✓ appena possibile, ogni altra informazione disponibile che venga richiesta dal TITOLARE in merito alla violazione dei dati personali.

Il RESPONSABILE può richiedere al TITOLARE un compenso ragionevole per servizi di assistenza che non sono compresi nella descrizione dei servizi e che non sono dovuti a errori, violazioni o condotte imputabili al RESPONSABILE.

COLLABORAZIONE CON LE AUTORITA' DI CONTROLLO

Il TITOLARE ed il RESPONSABILE cooperano, su richiesta, con l'autorità di controllo. Il TITOLARE è immediatamente informato di tutte le ispezioni e misure eseguite dall'autorità di controllo, nella misura in

cui esse si riferiscono alle attività svolte in base a questo Accordo. Ciò vale anche nel caso in cui il RESPONSABILE sia sottoposto a o coinvolto in una indagine da parte di un'autorità competente in relazione a violazioni di qualsiasi disposizione in materia di trattamento di dati personali nello svolgimento di attività ai sensi di questo Accordo. Nella misura in cui il TITOLARE sia soggetto a ispezione da parte dell'autorità di controllo, sanzione amministrativa pecuniaria, misura cautelare o procedimento penale, pretesa da parte di un interessato o di terzi o qualsiasi altra azione legale in collegamento con il trattamento di dati da parte del RESPONSABILE ai sensi della presente nomina, il RESPONSABILE farà tutto il possibile per sostenere il TITOLARE.

DIRITTI DEGLI INTERESSATI

Il RESPONSABILE si impegna a cooperare con il TITOLARE ed a fornire la più ampia assistenza, nei limiti in cui ciò è ragionevole o possibile, al fine di agevolare il TITOLARE nel riscontro delle richieste degli interessati per l'esercizio dei loro diritti.

In particolare, il RESPONSABILE si impegna a comunicare immediatamente al TITOLARE ciascuna richiesta pervenutagli dagli interessati in merito all'esercizio dei loro diritti e, se fattibile o del caso, ad assistere il TITOLARE nel progettare e implementare tutte le misure tecniche ed organizzative necessarie per rispondere a tali richieste.

Fermo restando che la responsabilità di riscontrare e soddisfare le richieste degli interessati grava esclusivamente sul TITOLARE, il RESPONSABILE può essere incaricato di evadere alcune specifiche richieste, sempre che ciò non richieda sforzi sproporzionati e su istruzioni specifiche fornite per iscritto dal TITOLARE.

POTERI DIRETTIVI DEL TITOLARE

Il RESPONSABILE non tratta alcun dato personale ai sensi del presente Accordo se non su istruzione documentata del TITOLARE, salvo che sia obbligato a farlo dal diritto dell'Unione o degli Stati membri.

Nel caso in cui il TITOLARE richieda una attività di trattamento dei dati personali non previsto dalle funzionalità del software e/o servizio SaaS, il RESPONSABILE informa immediatamente il TITOLARE qualora ritenga che tale richiesta possa comportare violazioni delle disposizioni in materia di protezione dei dati. Il RESPONSABILE può astenersi dallo svolgere qualsiasi attività che possa dar luogo a tale violazione.

Nel caso in cui il TITOLARE richieda attività di trattamento dei dati personali che comportino variazioni di risorse informatiche (inclusa modifica del codice) e organizzative non previste dal Contratto, AXIOS valuterà la fattibilità della richiesta e, se realizzabile, concorderà con il TITOLARE la specifica delle attività e i relativi costi, ovviamente, se le attività richieste non comportino violazioni delle disposizioni in materia di protezione dei dati.

POTERI DI CONTROLLO DEL TITOLARE

Il TITOLARE ha il diritto di svolgere ispezioni o farle svolgere ad un revisore di volta in volta incaricato. Il revisore dovrà valutare il rispetto di questo Accordo da parte del RESPONSABILE nel corso delle proprie attività d'impresa per mezzo di verifiche causali, le quali dovranno di regola essere notificate in anticipo.

Il RESPONSABILE deve permettere al TITOLARE di verificare l'adempimento alle proprie obbligazioni, come previsto dall'art. 28 RGPD. Su richiesta, il RESPONSABILE fornisce al TITOLARE ogni informazione necessaria nonché, segnatamente, la prova di aver adottato le misure tecniche ed organizzative.

Il RESPONSABILE può addebitare al TITOLARE un compenso di entità ragionevole per l'esecuzione delle ispezioni.

ALTRI RESPONSABILI DEL TRATTAMENTO (SUB-RESPONSABILI)

Il TITOLARE autorizza fin d'ora il RESPONSABILE a ricorrere a terzi responsabili del trattamento. I SUB-RESPONSABILI come richiesto dalla normativa, dovranno essere soggetti ai medesimi obblighi contrattuali contenuti nel presente Accordo ai sensi dell'art. 28 par. 4 dell'RGPD.

In virtù del presente Accordo, le parti si danno reciprocamente atto che il RESPONSABILE si avvale dei seguenti sub-responsabili, con i quali s'impegna a concludere accordi contrattuali conformi al dettato dell'art. 28, par. 4 dell'RGPD:

| | SUB-RESPONSABILE | INDIRIZZO/STATO | ATTIVITA' DI TRATTAMENTO DELEGATA |
|---|------------------|-------------------------------------------------------------|-----------------------------------------------------------------|
| 1 | Aruba S.p.A. | Via San Clemente n.53, 24036 Ponte San Pietro (BG) - ITALIA | Infrastruttura e servizi di Data Center |
| 2 | Aruba PEC S.p.A. | Via San Clemente n.53, 24036 Ponte San Pietro (BG) - ITALIA | Servizi di firma digitale grafometrica |
| 3 | MOMIT S.r.l. | Viale Enrico Forlanini n.23, 20134 Milano – ITALIA | Object Storage |
| 4 | Cloudflare, Inc. | 101 Townsend St, San Francisco, CA 94107 USA | Servizi di sicurezza Enterprise (localizzazione dei dati in UE) |

Resta inteso che la comunicazione dei dati ad un terzo responsabile potrà avvenire solo una volta che tutte le condizioni ai sensi dell'art.28 par.4 dell'RGPD siano realizzate.

Il RESPONSABILE manterrà aggiornato l'elenco dei SUB-RESPONSABILI. Qualsiasi modifica a tale elenco sarà segnalata al TITOLARE senza indebito ritardo.

Il RESPONSABILE risponde integralmente dell'operato dei SUB-RESPONSABILI nei confronti del TITOLARE.

Per i SUB-RESPONSABILI che prevedono il trasferimento dei dati al di fuori della UE/SEE, il RESPONSABILE garantisce la legittimità del trasferimento dati al di fuori dello SEE.

TRATTAMENTO ALL'ESTERNO DELLA UE E DELLO SEE

Alla data di stipula del presente accordo, il TITOLARE riconosce di essere stato informato che le attività di trattamento effettuate dal RESPONSABILE per suo conto, non prevedono trasferimenti al di fuori dello Spazio Economico Europeo "SEE". Se tali trattamenti, in questa sede specificamente autorizzati dal TITOLARE, dovessero in futuro richiedere il trasferimento di dati personali fuori dallo SEE, il RESPONSABILE farà in modo che i trattamenti avvengano in conformità alle basi di legittimità del trasferimento stabilite agli artt. 45 e ss. dell'RGPD, come di volta in volta applicabili a ciascun trattamento e fornirà al TITOLARE le informazioni necessarie senza indebito ritardo.

RESPONSABILITA'

Restano ferme le disposizioni di cui all'art. 82 RGPD.

DURATA DEL TRATTAMENTO, DISTRUZIONE E RESTITUZIONE DEI DATI PERSONALI

La durata del trattamento è limitata alla durata del Contratto di fornitura.

Il RESPONSABILE non crea copie o duplicati dei dati ad insaputa e senza il consenso del TITOLARE, fatta eccezione per le copie di sicurezza, nella misura in cui siano necessarie a garantire la corretta elaborazione dei dati (esecuzione del servizio), nonché per i dati la cui conservazione è prevista dalla legge.

A conclusione della prestazione dei servizi (termine del Contratto di fornitura), a scelta del TITOLARE, il RESPONSABILE cancella (rif. ALLEGATO "B") in maniera conforme alla protezione dei dati e restituisce al TITOLARE tutti i dati personali raccolti ed elaborati ai sensi del presente Accordo, a meno che le disposizioni di legge applicabili non richiedano un'ulteriore conservazione dei dati personali.

In ogni caso, il RESPONSABILE può conservare tutte le informazioni utili a dimostrare la corretta e conforme esecuzione delle attività di trattamento anche oltre la cessazione del Contratto.

La documentazione di cui al comma che precede, deve comunque essere conservata dal RESPONSABILE in ottemperanza ai periodi di conservazione previsti dalla legge o altrimenti stabiliti.

ALLEGATI

ALLEGATO "A" - CONDIZIONI DI LICENZA D'USO SOFTWARE AXIOS E RELATIVA ASSISTENZA

ALLEGATO "B" - POLICY DI SICUREZZA

Roma, 29/09/2022