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 RGDP - Regolamento Generale per la protezione dei Dati Personali) 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'RGDP;
- ✓ 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'RGDP, 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'RGDP 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
- ✓ Famigliari
- ✓ 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 RGDP. 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 RGDP. 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 RGDP, in particolare ai sensi dell'art. 5 par. 1 e par. 2 RGDP. 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 RGDP, 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 RGDP. 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 RGDP, 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 RGDP. 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'RGDP.

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'RGDP:

	SUB-RESPONSABILE	INDIRIZZO/STATO	ATTIVITA' DI TRATTAMENTO DELEGATA
1	Aruba S.p.A.	Via San Clemente n.53, 24036 Ponte San Pietro (BG) - ITALIA	Servizi tecnici
2	Aruba PEC S.p.A.	Via San Clemente n.53, 24036 Ponte San Pietro (BG) - ITALIA	Servizi di firma digitale e grafometrica
3	2C Solution S.r.l.	Via Martin Piva Artigiano n.12, 35010 Limena (PD)	Servizio di conservazione dei documenti informatici
4	MOMIT S.r.l.	Viale Enrico Forlanini n.23, 20134 Milano – ITALIA	Servizi tecnici

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 REPONSABILE 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'RGDP, 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 RGDP.

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, 11/01/2021

Si prega di consegnare il seguente documento
Al Dirigente Scolastico
Al Direttore dei Servizi Generali ed Amministrativi
Al Responsabile della Sicurezza

MISURE MINIME DI SICUREZZA

La circolare AgID del 26 Aprile 2016 in materia di "MISURE MINIME DI SICUREZZA ICT PER LE PUBBLICHE AMMINISTRAZIONI" deve essere vista come un documento utile a guidare le PA in un processo di conoscenza delle misure di sicurezza e della loro attuazione in base alla struttura delle singole PA.
Nei prossimi giorni uscirà una nota congiunta MIUR/AgID che spiegherà come il documento allegato alla circolare in oggetto e da compilare entro il 31/12/2017, non deve intendersi statico o impositivo, ma uno strumento per valutare la situazione della sicurezza nei sistemi informativi delle scuole e predisporre nel tempo gli adeguamenti necessari. Deve essere quindi visto come una guida alla cultura della sicurezza nelle scuole.
Axios intende da parte sua, con questa comunicazione, aiutare la compilazione del modello nei capitoli di propria competenza (ABSC 5 ed ABSC 10) delegando alla propria rete la consulenza da dare alle scuole per identificare e catalogare le peculiarità di ognuna.
E' evidente che questo documento, perché generico, non può tenere conto delle singole situazioni che devono essere indicate da ogni singola scuola.
Di seguito i capitoli riguardanti Axios e cosa, a nostro giudizio, dovrebbero contenere come informazioni.
Indicando i pacchetti Axios si intendono tutti i nostri prodotti Windows client/server, con l'indicazione invece di Axios Cloud, tutti i nostri programmi CLOUD (SD, RE e Protocollo)

All'interno della tabella "*ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE*" sono indicate ovviamente tutte le informazioni concernenti i prodotti Axios. E' importante ricordare come all'interno di tale tabella debbano essere indicati "*Regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi.*"
Come privilegi di amministratore non si intende solo l'amministratore dei programmi Axios ma qualsiasi altra utenza avente tali caratteristiche, dall'amministratore della macchina a quello di rete e del server.
Le indicazioni fornite quindi devono essere integrate con le informazioni circa la gestione delle utenze sopra descritte.
Esistono una serie di programmi free in internet che possono aiutare la scuola nella gestione di tali utenze al fine di rispettare quando indicato nella norma.

All'interno della tabella "*ABSC 10 (CSC 10): COPIE DI SICUREZZA*" devono essere indicati "*Procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità.*"
Uno degli strumenti più efficaci per garantire la sicurezza delle copie dei dati è sicuramente dato dal poter effettuare un backup su server cloud. Attenzione però perché questi devono in qualche modo essere certificati ed essere locati all'interno della Comunità Europea, in quanto, all'interno della base dati, sono presenti dati sia personali che sensibili.
Non è opportuno quindi utilizzare spazi cloud free, come forniscono molti giganti del WEB in quanto, pur perfettamente funzionanti, non garantiscono sicurezza e locazione geografica dei vostri backup.
Axios propone in questo caso ai propri clienti, al fine di essere tranquilli riguardo ad una procedura di Disaster Recovery, il proprio programma di Backup Cloud, completamente integrato ed automatizzato, che garantisce un elevato standard di sicurezza e protezione oltre ad una collocazione fisica dei server all'interno del territorio nazionale.

Programmi Axios Client/Server (seguire quanto indicato con il colore rosso)

Programmi Axios Cloud (seguire quanto indicato con il colore blue)
I programmi Axios in Cloud, Segreteria Digitale, Registro Elettronico e Protocollo WEB, così come i futuri sviluppi della tecnologia Axios in cloud sono installati e gestiti all'interno del data center di uno dei più grandi fornitori di servizi WEB collocato sul territorio nazionale: Aruba SpA.
Aruba si è dotata della certificazione ISO 27001:2013 e degli altri mezzi e/o strumenti ritenuti idonei a tutelare nella maniera più efficace la sicurezza delle informazioni (fisica, logica, informatica ed organizzativa). Il servizio da noi utilizzato è Server Dedicati, Housing e Colocation ed è certificato **ISO 9001:2008** per la qualità e **ISO 27001:2005** per la sicurezza.

ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE

ABSC_ID			Livello	Descrizione	Modalità di implementazione
5	1	1	M	Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.	I prodotti Axios consentono, per ogni utente ed ogni funzionalità, di indicare la tipologia di accesso possibile (CRUD). Il sistema Axios Cloud consente le medesime funzionalità.
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	I prodotti Axios registrano in automatico ogni accesso effettuato al sistema. Il sistema Axios Cloud possiede un log puntuale di tutte le operazioni effettuate e consente l'accesso allo stesso a qualsiasi richiesta proveniente dall'utente o dalle autorità preposte
5	1	3	S	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	Vedi punto 5.1.1M Anche per Axios Cloud vedi punto 5.1.1.M
5	1	4	A	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	I prodotti Axios registrano su tabella di log ogni singola operazione effettuata sui dati. La conservazione di tale log dipende dallo spazio presente sul disco del server della scuola e dalle impostazioni fornite dalla scuola stessa sulla grandezza massima del file di LOG. Il LOG gestito da Axios Cloud viene storicizzato ogni 3 mesi e collocato in stato di READONLY. Dopo 12 mesi viene cancellato
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	Tramite la gestione utenti di Axios è possibile verificare in qualsiasi momento lo status delle utenze, non ultima la data di ultimo accesso. Axios Cloud consente in ogni istante, da parte dell'amministratore di sistema, di verificare lo status delle utente.
5	2	2	A	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.	
5	3	1	M	Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.	
5	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	Vedi punto 5.1.4.A L'aggiunta o la soppressione di un'utenza amministrativa sono operazioni che vengono svolte sul DB e quindi regolarmente registrate nel file di LOG. Anche in Axios Cloud l'operazione viene regolarmente tracciata all'interno del file LOG.
5	4	2	S	Generare un'allerta quando viene aggiunta un'utenza amministrativa.	
5	4	3	S	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.	
5	5	1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	
5	6	1	A	Utilizzare sistemi di autenticazione a più fattori per tutti gli accessi amministrativi, inclusi gli accessi di amministrazione di dominio. L'autenticazione a più fattori può utilizzare diverse tecnologie, quali smart card, certificati digitali, one time password (OTP), token,	

				biometria ed altri analoghi sistemi.	
5	7	1	M	Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).	Axios consente di definire una serie di parametri che possono rendere sicure le credenziali di accesso ai propri programmi fornite: 1. Verifica o meno del doppio accesso 2. Inserimento data generale di scadenza password 3. Numero di gg massimi per la validità del codice di accesso 4. Numero massimo di gg da ultimo accesso per consentire ancora lo stesso 5. Lunghezza minima del codice di accesso (in questo caso 14) 6. Numero minimo dei caratteri minuscoli 7. Numero minimo dei caratteri maiuscoli 8. Numero minimo dei caratteri numerici 9. Numero minimo dei caratteri speciali In Axios Cloud verranno a breve implementate le stesse funzioni
5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	I parametri definiti in Axios al punto precedente (5.7.1.M) consentono di effettuare questo controllo in automatico impedendo di fatto l'utilizzo di credenziali deboli.
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	Vedi parametri indicati nel punto 5.7.1.M
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	Axios gestisce lo storico password impedendo di fatto che possa essere riutilizzato un codice di accesso già utilizzato in precedenza. In Axios Cloud sarà a breve implementata le medesima funzione
5	7	5	S	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.	
5	7	6	S	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	
5	8	1	S	Non consentire l'accesso diretto ai sistemi con le utenze amministrative, obbligando gli amministratori ad accedere con un'utenza normale e successivamente eseguire come utente privilegiato i singoli comandi.	Axios consente, per le funzioni particolarmente delicate, di inserire un ulteriore codice di accesso. L'utente quindi dopo aver effettuato il login dovrà inserire anche un ulteriore codice di accesso per poter effettuare la funzione scelta.
5	9	1	S	Per le operazioni che richiedono privilegi gli amministratori debbono utilizzare macchine dedicate, collocate su una rete logicamente dedicata, isolata rispetto a Internet. Tali macchine non possono essere utilizzate per altre attività.	
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	La gestione degli amministratori rispetto alle normali utenze viene fatta, in Axios, tramite la gestione dei livelli (1-9 9=amministratore) e le tipologie di accesso per ogni utente/funzione (5.1.1M)
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	In Axios, ad ogni utenze, è legata la relativa anagrafica del personale gestita all'interno dei programmi stessi Anche in Axios Cloud le utenze di accesso sono legate a precise anagrafiche presenti nel sistema
5	10	3	M	Le utenze amministrative anonime, quali "root" di UNIX o	

				"Administrator" di Windows, debbono essere utilizzate solo per le situazioni di emergenza e le relative credenziali debbono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso.	
5	10	4	S	Evitare l'uso di utenze amministrative locali per le macchine quando sono disponibili utenze amministrative di livello più elevato (e.g. dominio).	
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	Per quanto concerne i prodotti Axios tali credenziali sono gestite all'interno della base dati, l'accesso alla stessa è consentito solo tramite i programmi Axios e quindi secondo le regole di sicurezza enunciate in questo documento. Anche per Axios Cloud vale lo stesso principio con l'aggiunta che la base dati non è in alcun modo accessibile a nessuno se non tramite programmi Axios e quindi secondo le regole indicate nel presente documento.
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	

ABSC 10 (CSC 10): COPIE DI SICUREZZA

ABSC_ID			Livello	Descrizione	Modalità di implementazione
10	1	1	M	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.	Il programma Axios prevede un sistema automatico e non presidiato di copie del proprio DB presente localmente sul server della scuola. Il sistema prevede inoltre l'invio automatico a tre indirizzi mail e/o a tre numeri di cellulare, di un messaggio sull'esito dell'esecuzione delle copie. Il sistema di backup Axios prevede anche la possibilità di effettuare un backup non solo della base dati ma anche di una specifica cartella condivisa sul server della scuola stessa e tutte le sue sottocartelle. Axios Cloud effettua - Backup del logo delle transazioni ogni 30 minuti - Backup completo ogni giorno alle 2.00 circa - Retention dei backup 8/10 gg
10	1	2	A	Per assicurare la capacità di recupero di un sistema dal proprio backup, le procedure di backup devono riguardare il sistema operativo, le applicazioni software e la parte dati.	Per quanto concerne Axios il sistema di backup effettua il salvataggio della base dati. L'installazione dei programmi è possibile in qualsiasi momento dal sito internet di Axios, così come l'eventuale ripristino del motore di database utilizzato (Sybase ver. 8.0.2.4495) Axios Cloud oltre ad esser dotato di un sistema di backup con retention di 8/10gg dei dati ed un sistema di retention di 2/4 gg delle immagini dell'intera infrastruttura e configurato con un sistema di DR Real Time che consente il ripristino di un subset depotenziato dell'infrastruttura madre entro 24/48 ore dal Fault completo del sistema principale garantendo, quindi, la continuità di servizio con uno SLA del 98.98 % circa
10	1	3	A	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	Axios consente alle scuole di poter effettuare, nella medesima sessione di copie ed in modo completamente automatico, oltre alla copia sul disco del server, anche una copia su unità fisica esterna e, qualora la scuola abbia acquistato il servizio, anche un backup cloud che garantisce l'assoluta salvaguardia e recuperabilità dei dati. I backup Axios Cloud sono conformi a tutte le regole attuali per il Disaster Recovery
10	2	1	S	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	Axios effettua una verifica al termine della creazione del file compresso contenente le copie. La simulazione del ripristino dei dati è comunque buona pratica da adottare con frequenza almeno mensile.
10	3	1	M	Assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. La codifica effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud.	Il backup effettuato da Axios è un file ZIP criptato che può essere ripristinato solo dalla scuola che lo ha generato. Questo consente di rimanere a norma anche con l'utilizzo di Backup Cloud di Axios. Axios Cloud consente l'accesso ai dati solo ai legittimi proprietari degli stessi. Tutte le transazioni Axios Cloud sono cifrate e protette da protocollo HTTPS

10	4	1	M	Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.	Vedi quanto indicato nel punto 10.1.3.A, in particolare è possibile effettuare una copia su un disco esterno, ad esempio, e poi isolare quest'ultimo dal sistema semplicemente scollegando il cavo dal server. I backup Axios Cloud sono conformi a tutte le regole attuali per il Disaster Recovery

Privacy Policy – Informativa sul trattamento dei dati personali ai sensi dell'art.13 del Regolamento UE 2016/679

Premessa

Axios Italia Service Srl SU con sede in Via Emanuele Filiberto n.190, 00185 Roma, Codice Fiscale e Partita IVA 06331261005, in qualità di Titolare del trattamento (di seguito "Titolare"), ai sensi del Regolamento UE 2016/679 (di seguito "Regolamento"), considera la privacy e la tutela dei dati personali un pilastro fondamentale nella propria attività.

La invitiamo, dunque, prima di comunicare qualsiasi dato personale al Titolare, a leggere con attenzione la presente Privacy Policy perché contiene informazioni importanti sulla tutela dei Suoi dati personali.

La presente Privacy Policy:

- ✓ si intende resa per il sito https://www.axiositalia.it/ (d'ora in avanti: "Sito");
- ✓ costituisce parte integrante del Sito e dei servizi che offriamo;
- ✓ è resa, ai sensi dell'art.13 del Regolamento, a coloro che interagiscono con i servizi web del Sito, sia mediante la semplice consultazione che mediante l'utilizzo di specifici servizi messi a disposizione tramite il Sito.

Questo documento è stato redatto ai sensi dell'art.13 del Regolamento al fine di permetterle di conoscere la nostra politica sulla privacy, per capire come le Sue informazioni personali vengono gestite quando utilizza il nostro Sito e, nel caso, di prestare un consenso al trattamento dei Suoi dati personali espresso e consapevole. Le informazioni ed i dati da Lei forniti od altrimenti acquisiti nell'ambito dell'utilizzo dei servizi di Axios Italia Service Srl SU, come ad esempio l'assistenza tecnica applicativa, la formazione on line o l'organizzazione di eventi (di seguito "Servizi"), saranno oggetto di trattamento nel rispetto delle disposizioni del Regolamento e degli obblighi di riservatezza che ispirano l'attività della Axios Italia Service Srl SU.
Secondo le norme del Regolamento, i trattamenti effettuati dalla Axios Italia Service Srl SU saranno improntati ai principi di liceità, correttezza, trasparenza, limitazione delle finalità e della conservazione, minimizzazione dei dati, esattezza, integrità e riservatezza.

Titolare del trattamento

Il Titolare del trattamento è la Axios Italia Service Srl SU con sede in Via Emanuele Filiberto n.190, 00185 Roma, Codice Fiscale e Partita IVA 06331261005, raggiungibile agli indirizzi mail: privacy@axiositalia.com e axios@aziendemail.it (PEC)

Responsabile per la Protezione dei Dati "DPO"

Il Responsabile per la Protezione dei Dati designato è il Sig. Vincenzo De Vita raggiungibile all'indirizzo mail: dpo@axiositalia.com

Tipologia di dati trattati

A seguito della navigazione del Sito, La informiamo che Axios Italia Service Srl SU tratterà i Suoi dati personali che potranno essere costituiti da: un identificativo come il nome, un numero di identificazione, un identificativo online o uno o più elementi caratteristici della Sua identità fisica, economica, culturale o sociale idonea a rendere il soggetto interessato identificato o identificabile (di seguito solo "Dati Personali").
I Dati Personali trattati attraverso il Sito sono i seguenti:

- Dati di contatto quali nome, cognome, e-mail e numero di telefono.

Potrebbero essere trattati dati particolari da Lei liberamente forniti in una mail di richiesta informazioni.

a. Dati di navigazione

I sistemi informatici e le procedure software preposte al funzionamento del Sito acquisiscono, nel corso del loro normale esercizio, alcuni Dati Personali la cui trasmissione è implicita nell'uso dei protocolli di comunicazione di Internet. Si tratta di informazioni che non sono raccolte per essere associate a interessati identificati, ma che per loro stessa natura potrebbero, attraverso elaborazioni ed associazioni con dati detenuti da terzi, permettere di identificare gli utenti. In questa categoria di dati rientrano gli indirizzi IP o i nomi a dominio dei computer utilizzati dagli utenti che si connettono al Sito, gli indirizzi in notazione URI (Uniform Resource Identifier) delle risorse richieste, l'orario della richiesta, il metodo utilizzato nel sottoporre la richiesta al server, la dimensione del file ottenuto in risposta, il codice numerico indicante lo stato della risposta data dal server (buon fine, errore, etc.) ed altri parametri relativi al sistema operativo e all'ambiente informatico dell'utente. Questi dati vengono utilizzati al solo fine di ricavare informazioni statistiche anonime sull'uso del Sito e per controllarne il corretto funzionamento, per identificare anomalie e/o abusi, e vengono cancellati immediatamente dopo l'elaborazione. I dati potrebbero essere utilizzati per l'accertamento di responsabilità in caso di ipotetici reati informatici ai danni del Sito o di terzi; salva questa eventualità, allo stato i dati sui contatti web non persistono per più di 90 giorni.

b. Speciali categorie di dati personali

Nell'invio di richieste di consulenza mezzo mail, potrebbe verificarsi un conferimento di Suoi Dati Personali rientranti nel novero delle speciali categorie di Dati Personali di cui all'art. 9 del Regolamento, testualmente i "[…] dati idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona". La invitiamo a comunicare tali dati solo ove strettamente necessario. Invero, Le ricordiamo che a fronte della trasmissione di speciali categorie di Dati Personali, ma in assenza di specifica manifestazione del consenso a trattare tali dati (eventualità che comunque Le consente ovviamente di inviare un curriculum vitae), la Axios Italia Service Srl SU non potrà essere ritenuta responsabile a nessun titolo, né potrà ricevere contestazioni di sorta, poiché in tal caso il trattamento sarà consentito in quanto avente ad oggetto dati resi manifestamente pubblici dall'interessato, in conformità con l'art. 9(2)(e) del Regolamento. Specifichiamo comunque l'importanza, come sopra già segnalato – di manifestare

l'esplicito consenso al trattamento delle speciali categorie di Dati Personali, laddove decidesse di condividere tali informazioni.

c. Dati forniti volontariamente dall'interessato

Nell'utilizzo di alcuni Servizi del Sito potrebbe verificarsi un trattamento di Dati Personali di terzi soggetti da Lei inviati ad Axios Italia Service Srl SU. Rispetto a tali ipotesi, Lei si pone come autonomo titolare del trattamento, assumendosi tutti gli obblighi e le responsabilità di legge. In tal senso, conferisce sul punto la più ampia manleva rispetto ad ogni contestazione, pretesa, richiesta di risarcimento del danno da trattamento, ecc. che dovesse pervenire ad Axios Italia Service Srl SU da terzi soggetti i cui Dati Personali siano stati trattati attraverso il Suo utilizzo delle funzioni del Sito in violazione delle norme sulla tutela dei dati personali applicabili. In ogni caso, qualora fornisse o in altro modo trattasse Dati Personali di terzi nell'utilizzo del Sito, garantisce fin da ora – assumendosene ogni connessa responsabilità – che tale particolare ipotesi di trattamento si fonda su un'idonea base giuridica ai sensi dell'art. 6 del Regolamento che legittima il trattamento delle informazioni in questione.

Finalità del trattamento

I dati personali saranno trattati per le seguenti finalità:

- ✓ Consentire l'erogazione dei Servizi richiesti quali:
  a) Iscrizione alla newsletter via e-mail;
  b) Richiesta generica di informazioni (incluse eventuali offerte);
  c) Iscrizione a corsi di formazione, eventi ed iniziative organizzate da Axios Italia Service Srl SU;
  d) Richieste di assistenza tecnica o consulenza;
  e) Assolvere eventuali obblighi di legge, contabili e fiscali.

Base giuridica e natura obbligatoria o facoltativa del trattamento

La base legale del trattamento di Dati Personali per le finalità di cui ai punti a), b), c), d) è l'art. 6(1)(b) del Regolamento in quanto i trattamenti sono necessari all'erogazione dei Servizi o per il riscontro di richieste dell'interessato. Il conferimento dei Dati Personali per queste finalità è facoltativo ma l'eventuale mancato conferimento comporterebbe l'impossibilità di attivare i Servizi forniti dal Sito. La finalità di cui al punto e), rappresenta un trattamento legittimo di Dati Personali ai sensi dell'art. 6(1)(c) del Regolamento. Una volta conferiti i Dati Personali, il trattamento è invero necessario per adempiere ad un obbligo di legge a cui la Axios Italia Service Srl SU è soggetta.

Per i trattamenti effettuati ai fini di invio diretto di proprio materiale pubblicitario o di propria vendita diretta o per il compimento di proprie ricerche di mercato o di comunicazioni commerciali in relazione a prodotti o Servizi di Axios Italia Service Srl SU analoghi a quelli da Lei richiesti, Axios Italia Service Srl SU può utilizzare, senza il Suo consenso, gli indirizzi di posta elettronica e di posta cartacea ai sensi e nei limiti consentiti dal provvedimento dell'Autorità Garante per la protezione dei dati personali del 19 giugno 2008; la base giuridica del trattamento dei Suoi dati per tale finalità è l'art. 6(1)(f) del Regolamento.

In ogni caso, ai sensi dell'art. 21 del Regolamento, Lei ha la possibilità di opporsi a tale trattamento in ogni momento, inizialmente o in occasione di successive comunicazioni, in maniera agevole e gratuitamente anche scrivendo al

Titolare o al DPO ai recapiti sopra indicati, nonché di ottenere un immediato riscontro che confermi l'interruzione di tale trattamento (art. 15 del Regolamento).

Destinatari dei dati personali

Esclusivamente per le finalità sopra indicate, i dati saranno resi disponibili, oltre che al personale interno autorizzato, anche a collaboratori esterni incaricati del loro trattamento il cui elenco è disponibile presso la sede del Titolare.

I dati personali non verranno diffusi, con tale termine intendendosi il darne conoscenza a soggetti indeterminati in qualunque modo, anche mediante la loro messa a disposizione o consultazione.

Criteri di Conservazione dei dati

I dati saranno conservati da Axios Italia Service Srl SU per tutto il periodo necessario all'erogazione dei Servizi richiesti, per i tempi successivi necessari a adempiere alle norme di legge, nonché per i tempi necessari per permettere un'eventuale difesa e tutela in giudizio.

Trasferimento dei dati in Paesi Extra UE

Non è previsto il trasferimento dei dati in Paesi terzi al di fuori della comunità europea. Esclusivamente per le finalità di corsi di formazione e eventi in videoconferenza, viene utilizzato il servizio GoToMeeting di **LogMeIn** relativamente al quale si consiglia la lettura della informativa sulla privacy.

Processi automatizzati di profilazione

I dati conferiti non sono oggetto di processi decisionali automatizzati.

Diritti degli interessati

L'interessato ha diritto ad esercitare i propri diritti secondo quanto previsto dagli artt.15-22 del Reg. UE 2016/679. Pertanto, i soggetti cui si riferiscono i dati personali hanno il diritto in qualunque momento di ottenere la conferma dell'esistenza o meno dei medesimi dati e di conoscerne il contenuto e l'origine, verificarne l'esattezza o chiederne l'integrazione o l'aggiornamento, oppure la rettificazione, la cancellazione, la portabilità, la trasformazione in forma anonima o il blocco in violazione di legge, nonché di opporsi in ogni caso, per motivi legittimi, al loro trattamento.

Le richieste vanno rivolte:

- ✓ via e-mail all'indirizzo: privacy@axiositalia.com;
- ✓ via posta ad Axios Italia Service Srl SU, 00185 Roma – Via Emanuele Filiberto, 190.

In particolare, per l'eventuale servizio facoltativo di newsletter, l'utente potrà anche richiedere la cancellazione dell'iscrizione in una delle seguenti modalità alternative: seguendo le istruzioni inserite in fondo ad ogni newsletter, alla voce "Cancella l'iscrizione" oppure inviando una mail all'indirizzo marketing@axiositalia.com indicando come oggetto "Cancella iscrizione newsletter".

I diritti degli interessati, inoltre, sono tutelati dall'Autorità di Controllo a cui è possibile, in caso di necessità, proporre reclamo (Garante per la protezione dei dati personali Piazza Venezia n.11 - 00187 ROMA Fax: (+39) 06.69677.3785 Centralino telefonico: (+39) 06.696771 E-mail: garante@gpdp.it Posta certificata: protocollo@pec.gpdp.it).

Aggiornamento della Privacy Policy

La presente privacy policy è in vigore dal 29 settembre 2020. Axios Italia Service Srl SU si riserva di modificarne o semplicemente aggiornarne il contenuto, in parte o completamente, anche a causa di variazioni della normativa applicabile. La Axios Italia Service Srl SU La informerà di tali variazioni non appena verranno introdotte ed esse saranno vincolanti non appena pubblicate sul Sito. La Axios Italia Service Srl SU La invita quindi a visitare con regolarità questa sezione per prendere cognizione della più recente ed aggiornata versione della privacy policy in modo da essere sempre aggiornato sui dati raccolti e sull'uso che ne fa la Axios Italia Service Srl SU.

Il Titolare del trattamento
Axios Italia Service S.r.l. S.U.
L'Amministratore Unico
Stefano Rocchi