



Ministero dell'istruzione, dell'Università e della Ricerca

Istituto Comprensivo Grosio - Grosotto - Sondalo

Piazzale Rinaldi 1 – 23033 Grosio (SO)

Tel: 0342/887595 - e-mail: soic82400v@istruzione.it soic82400v@pec.istruzione.it

www.icgrosiogrosottosondalo.gov.it - Codice fiscale 93028000144

Prot. n. 81/51/1.4.a

**CONTRATTO DI NOMINA A RESPONSABILE DEL TRATTAMENTO DEI DATI
AI SENSI DELL'ART. 28 REG. UE 2016/679 ("GDPR")**

Il presente contratto viene stipulato tra l'Istituto Comprensivo di Grosio Grosotto Sondalo con sede legale in Grosio (SO), Piazzale Rinaldi, 1 e Swisstech S.r.l. con sede legale in Pordenone (PN), Piazza del Cristo, 12, in ottemperanza a quanto previsto dall'art. 28 del Regolamento UE 2016/679, d'ora in poi per brevità denominato GDPR.

1. Oggetto

Il presente contratto disciplina i trattamenti di dati effettuati da Swisstech S.r.l., in qualità di responsabile del trattamento designato con il presente atto dall'Istituto Comprensivo di Grosio Grosotto Sondalo ai sensi dell'art. 28 del GDPR, per le seguenti finalità:

Responsabile esterno del trattamento dei dati, ai sensi dell'art. 28 del GDPR

per dare seguito al contratto di servizio di seguito riportato:

Contratto Responsabile Trattamento dati Prot. n. 8151/6.9.a

Ai fini del presente contratto, Swisstech S.r.l. assume pertanto anche la qualifica di "Fornitore" di servizi.

2. Posizione di SWISSTECH S.r.l. : "Fornitore"

Ai fini del presente contratto, ed in ottemperanza a quanto previsto dall'art. 28 del GDPR, Swisstech S.r.l. assume la qualifica di responsabile del trattamento dei dati, e di conseguenza si configura come "Fornitore" di servizi nei confronti del titolare. Nel resto del presente atto pertanto Swisstech S.r.l. potrà venire qualificata come "Fornitore"

3. Ottemperanza alla normativa in materia di sicurezza e protezione dei dati, con particolare riferimento al Reg. UE 2016/679 - GDPR

Ai fini del presente contratto, Swisstech S.r.l. si impegna ad ottemperare a tutte le prescrizioni, a livello nazionale ed europeo, in materia di sicurezza e protezione dei dati personali; in particolare Swisstech S.r.l. si impegna ad osservare tutte le prescrizioni del Regolamento UE 2016/679, ed a comunicare al titolare, in ottemperanza al principio di responsabilizzazione ("accountability") le concrete modalità di adeguamento al GDPR. In particolare Swisstech S.r.l. si impegna a comunicare al titolare le concrete modalità e passi operativi attraverso i quali Swisstech S.r.l. mette in atto, in ottemperanza a quanto prescritto dall'art. 32 comma 1 lettera b) del GDPR, "*una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative al fine di garantire la sicurezza del trattamento*".

4. Divieto di subappalto o subfornitura se non esplicitamente approvato dal titolare

In ottemperanza a quanto previsto dall'art. 28 comma 2 del GDPR, il responsabile/fornitore non ricorre ad altro responsabile senza previa autorizzazione scritta del titolare. Qualsiasi ricordo ad altri sub-responsabili da parte del responsabile, dovrà pertanto essere preventivamente autorizzata per iscritto dal titolare.

5. Fornitura dei Registri del trattamento

Qualora il responsabile rientri nella casistica prevista dall'art. 30 del GDPR, ed in particolare qualora il responsabile sia una impresa od organizzazione con più di 250 dipendenti, il responsabile è tenuto a comunicare al titolare i Registri delle attività di trattamento svolte per conto del titolare.

6. Personale del Fornitore e Riservatezza

Il Fornitore dichiara e garantisce che, nell'ambito della propria organizzazione e di eventuali sub-responsabili, i dati personali saranno trattati solo da persone appositamente autorizzate e designate per iscritto, vincolate ad una condotta equivalente al segreto professionale ed al segreto d'ufficio, ed hanno ricevuto precise istruzioni scritte in merito alle prassi da seguire nelle operazioni di trattamento dei dati. Il fornitore si impegna a comunicare al titolare le istruzioni impartite ai soggetti designati al trattamento dei dati.

7. Operazioni di Amministrazione e Gestione di Sistema

Il Fornitore si impegna ad ottemperare in maniera autonoma a tutte le prescrizioni del Provvedimento del Garante per la protezione dei dati personali del 27-11-2008 e successive mm. ii., ed in particolare per quanto riguarda i soggetti sia interni che esterni che agiscono con la qualifica di amministratore di sistema o equivalente, dichiara di aver previamente valutato l'esperienza, le capacità e l'affidabilità dei soggetti designati, i quali devono fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza.

Il Fornitore pertanto si impegna:

- a istituire e mantenere aggiornato uno schema ed un inventario dei sistemi
- ad attivare o far attivare, per ciascuno dei sistemi di cui al punto precedente, idonei meccanismi di tracciatura ("logging") degli accessi effettuati con profilo di amministratore nonché delle operazioni effettuate, con modalità che permettano di avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi
- a comunicare al titolare i suddetti file di log con frequenza trimestrale, od ogniqualvolta il titolare ne faccia richiesta
- ad individuare nominativamente per iscritto gli amministratori di sistema, specificando l'ambito del trattamento consentito e le credenziali di admin associate, che devono essere assegnate ed utilizzate su base nominativa individuale.

8. Sicurezza dei dati personali

In ottemperanza a quanto previsto dall'art. 32 del GDPR, tenuto conto della tipologia di dati (dati sensibili e relativi allo stato di salute) e dei rischi connessi, il titolare impone al responsabile/fornitore che i dati informato elettronico siano cifrati, con procedure di cifratura di adeguata robustezza ed inviolabilità.

Il titolare impone inoltre che i dati siano trattati mettendo in atto misure tecniche ed organizzative che permettano di assicurare su base permanente la riservatezza, l'integrità, la disponibilità dei dati.

Il responsabile/fornitore è tenuto a mettere in atto un procedura per testare, verificare e valutare periodicamente l'efficacia delle misure tecniche ed organizzative al fine di garantire la sicurezza del trattamento.

Si chiede quindi al fornitore di comunicare al titolare quale sia in concreto (metodologia, ruoli, passi operativi, tecniche, strumenti etc.) la procedura operativa di cui al punto precedente, e con che frequenza essa venga messa in atto.

9. Violazione dei dati

Il fornitore si impegna a comunicare per iscritto al titolare, tempestivamente a comunque non oltre le 24h da momento in cui ne è venuto a conoscenza, qualsiasi violazione dei dati che riguardi i dati detenuti dal fornitore o da qualsiasi sub-responsabile.

Al fine di consentire al titolare di ottemperare a quanto previsto dal GDPR, la comunicazione di cui sopra dovrà contenere almeno le seguenti informazioni:

- descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- descrivere le probabili conseguenze della violazione dei dati personali;
- descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

10. Registro delle violazioni dei dati

Il responsabile/fornitore è tenuto in ogni caso a istituire e tenere regolarmente aggiornato un registro delle violazioni dei dati, ai sensi ed in ottemperanza a quanto prescritto dall'art. 33 comma 5 del GDPR. Detto registro deve essere esibito in caso di verifiche od ispezioni presso la struttura del fornitore da parte del titolare o di soggetti da questo delegati.

11. Data Protection Impact Assessment

Tenuto conto del fatto che quando un tipo di trattamento, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, nel caso i trattamenti di dati rientrino nelle casistiche previste dall'art. 35, o comunque nel caso lo richieda il titolare, il fornitore è tenuto ad effettuare una valutazione d'impatto sulla protezione dei dati, nei modi prescritti dall'art. 35 del GDPR. Detta valutazione d'impatto dovrà essere sottoposta alla valutazione da parte del titolare, il quale dovrà verificare la completezza, l'accuratezza e la conformità alla metodologia imposta dall'art. 35 comma 7 del GDPR.

12. Ispezioni e Audit

Il titolare ha facoltà di vigilare anche tramite ispezioni e verifiche periodiche, sulla puntuale osservanza delle prescrizioni impartite al responsabile / fornitore nel presente documento e più in generale sull'osservanza a quanto prescritto dall'art. 28 del GDPR.

13. Sanzioni penali e obbligo di risarcimento del danno causato

Il responsabile/fornitore è a conoscenza del fatto che in caso di non ottemperanza alle prescrizioni del presente contratto e più in generale delle prescrizioni del Reg. UE 2016/679, le sanzioni amministrative pecuniarie possono arrivare fino a 20.000.000,00 Euro. In ogni caso incombe sul responsabile l'obbligo di risarcire il danno causato come effetto del trattamento dei dati, ai sensi dell'art. 82 del GDPR.

14. Durata del contratto

La durata del presente contratto segue la durata contratto di servizio. Potrà però in qualsiasi momento essere rescisso da parte del titolare in caso di grave inadempienza del responsabile alle prescrizioni contenute nel presente documento.

15. Gestione dei dati alla fine del contratto

All'atto della conclusione o revoca del contratto, il responsabile si impegna ad attenersi scrupolosamente alle istruzioni che saranno impartite dal titolare in merito alla gestione dei dati .

GROSIO, 23 Giugno 2018

I.C. GROSIO GROSOTTO SONDALO

SWISSTECH S.R.L.

Per accettaz. di tutte le clausole del presente contratto
