PROTOCOLLO DI INTESA
Data Protection Officer (DPO)
Anno scolastico 2018/2019

PREMESSO CHE

La nota MIUR n. 563/2018 "*Regolamento generale sulla protezione dei dati (UE/2016/679)*" specifica che il Regolamento Europeo in materia di protezione dei dati personali (GDPR) attribuisce ai soggetti pubblici una significativa discrezionalità nell'individuazione delle modalità organizzative di adeguamento alle novità previste.

Ciascun istituto scolastico deve dotarsi, in via prioritaria, del ***Responsabile della protezione dei dati personali***, il quale deve possedere i requisiti di autonomia e indipendenza, operare senza conflitto di interessi e possedere specifiche competenze in materia di trattamento dei dati personali.

Tenendo conto della previsione dell'art. 37, comma 3 del Regolamento, è consentito a più scuole di avvalersi di un unico Responsabile dei dati per le autorità pubbliche. L'atto di designazione di un unico Responsabile potrà avvenire attraverso la decisione congiunta di scuole già costituite in reti di scopo poste in essere per l'attuazione di procedure amministrative di interesse comune.

CONSIDERATO CHE

Eurosofia è soggetto qualificato dal MIUR per la formazione del personale della Scuola ai sensi della direttiva n. 170/2016 ed è presente nella piattaforma ministeriale S.O.F.I.A.

Udir, nel corso del Convegno Nazionale che si è tenuto a Palermo il 19/05/2018, ha affrontato il tema dell'adeguamento al "Regolamento generale sulla protezione dei dati (UE/2016/679)" e si impegna ad attivare il percorso di adeguamento delle istituzioni scolastiche ai sensi del nuovo Regolamento sul trattamento dei dati, attraverso anche la nomina di un Data Protection Officer altamente qualificato che possa tutelare le scuole.

CIO' PREMESSO E CONSIDERATO

UDIR, in virtù dei rapporti di collaborazione con Eurosofia, propone una particolare ***convenzione con una società di servizi specializzata e altamente qualificata in materia***.

In particolare il ***Servizio di Assistenza consulenza privacy e DPO*** proposto si articola in diverse fasi, volte a garantire alla scuola un servizio di consulenza per tutto l'arco della durata del contratto, attraverso il sostegno di uno o più tecnici dedicati che seguiranno sia direttamente presso la sede, sia attraverso il lavoro in ufficio e l'assistenza telefonica o telematica (es. mail)

- ***Consulenza Privacy | Modello organizzativo Sicurezza Privacy (MOSP) | Workflow Privacy***

- *Studio della realtà aziendale*
- *Redazione di un Modello Organizzativo Privacy e di un Workflow dei trattamenti privacy*
- *Aggiornamento informative ai sensi degli art. 13/14 del Regolamento (UE) 2016/679*
- *Mappatura misure di sicurezza ex art. 32 GDPR*
- *Informazione sui possibili rischi connessi alla non applicazione della legge*
- *Consegna documentale*

- ***Privacy | Ruoli e Responsabilità interni e esterni***

- *Aggiornamento individuazione responsabili esterni ai sensi degli art. 28 del Regolamento (UE) 2016/679*
- *Aggiornamento individuazione delegati privacy interni ed incaricati ai sensi degli art. 29 del Regolamento (UE) 2016/679*
- *Individuazione e nomina Amministratori di Sistema*
- *Eventuale individuazione del Responsabile della Protezione dei Dati (RPD \| DPO) \| Data Protection Officer e predisposizione nomina ai sensi degli artt. 37 – 38 – 39 Reg. (UE) 2016/679*
- *Redazione e aggiornamento organigramma Privacy interno*

- ***Registro delle attività del Titolare del Trattamento***

Ai sensi dell'art.30 c. 1 del Regolamento generale sulla Protezione dei dati (Regolamento (UE) 2016/679 verrà strutturato e reso disponibile un elenco in formato elettronico o cartaceo dei trattamenti del Titolare svolte sotto la propria

responsabilità e, ove applicabile del suo rappresentante.

Nel caso in cui si richieda invece un documento attraverso un tool in web application o locale su client, Vi verrà predisposta apposita offerta.

- ***Registro delle attività del Responsabile del Trattamento***

Ai sensi dell'art.30 c. 2 del Regolamento generale sulla Protezione dei dati (Regolamento (UE) 2016/679 verrà strutturato e reso disponibile un elenco in formato elettronico o cartaceo dei trattamenti del Responsabile svolte per conto del Titolare e, ove applicabile del suo rappresentante.

Nel caso in cui si richieda invece un documento attraverso un tool in web application, Vi verrà predisposta apposita offerta.

- ***Redazione di procedura Violazione dei dati personali e registrazione eventi | Data Breach***

Gli artt. 33 e 34 del Regolamento (UE) 2016/679 GDPR richiedono che il Titolare del trattamento debba gestire correttamente i casi di violazione di dati personali e che debba – art. 33 c. 5 GDPR – documentare qualsiasi violazione di dati personali con i relativi provvedimenti. Verrà quindi predisposta una policy di data breach che permetta di coinvolgere le funzioni responsabili del trattamento e se istituito il servizio di DPO è istituito un registro per la registrazione degli eventi.

- ***Predisposizione policy sulla conservazione dei dati | Data Retention Policy***

Ai sensi degli Art. 5,13,14 del Regolamento (UE) 2016/679 verrà redatta una policy sui tempi di conservazione dei dati diversificata per tipologie di trattamento

- ***Privacy Impact Assessment | Valutazione d'impatto (art. 35 GDPR)***

Redazione di una valutazione di impatto per i trattamenti ricadenti nella disciplina dell'art. 35 del Regolamento Privacy UE e ricompresi nell'elenco delle tipologie di trattamento soggette e pubblicate dall'Autorità di controllo (in fase di pubblicazione).

Il documento è obbligatorio quando i trattamenti riguarderanno nuove tecnologie e presenteranno rischi elevati per gli interessati in relazione alla natura, il campo di applicazione, il contesto e finalità di trattamento, per i diritti e le libertà delle persone fisiche.

- ***Consulenza sul provvedimento del Garante Privacy sugli Amministratori di Sistema Informatici (AdS) al fine di applicare il Provvedimento del Garante Privacy del 27 novembre 2008 (G.U. n. 300 del***

24 dicembre 2008, così modificato in base al provvedimento del 25 giugno 2009 G.U. n. 149 del 30 giugno 2009) che prevede:

- *Consulenza nell'individuazione degli Amministratori di Sistema interni ed esterni alla Vostra struttura e valutazione dei requisiti*
- *Predisposizione nomine degli Amministratori di Sistema e/o manutentori occasionali e/o /Responsabili del trattamento*
- *Linee guida per la verifica annuale degli Amministratori di Sistema*
- *Predisposizione dell'elenco degli Amministratori di Sistema e indicazioni su come renderlo noto ai dipendenti*
- *Indicazioni circa la registrazione dei file di log degli accessi degli Amministratori di Sistema, ove obbligatorio*

❖ ***Stesura/Adeguamento del regolamento sul corretto utilizzo degli Strumenti Informatici aziendali ai sensi delle linee guida del Garante privacy per posta elettronica e internet | G.U. n. 58 del 10 marzo 2007) e art. 4 della L. 300/70 come modificato dal D. lgs. 151/2015 ("Jobs act")***

- *Stesura/aggiornamento del Regolamento interno per l'utilizzazione di strumenti aziendali (computer, posta elettronica, internet, mobile device) ai sensi del provvedimento del Garante del 1° marzo 2007 e alla luce del art. 4 della L. 300/70 come modificato dal D. lgs. 151/2015 ("Jobs act") e dell'Opinion 2/2017 WP29 | "on data processing at work"*

❖ ***Consulenza sul provvedimento del Garante Privacy in tema di videosorveglianza del 08 aprile 2010 pubblicato sulla Gazzetta Ufficiale n° 99 il 29 aprile 2010 e art. 4 della L. 300/70 come modificato dal D. lgs. 151/2015 ("Jobs act")***

- *Predisposizione e fornitura della documentazione necessaria per la messa a norma rispetto agli adempimenti del Provvedimento dell'aprile 2010 dell'Autorità Garante Privacy sulla Videosorveglianza anche alla luce del art. 4 della L. 300/70 come modificato dal D. lgs. 151/2015 ("Jobs act")*

❖ ***Verifica Sito Internet e Consulenza ai sensi del Provvedimento del Garante Privacy sui cookies***

- *Verifica, attraverso la predisposizione di informative art. 13 T.U. (privacy policy) e consensi, del corretto utilizzo e della corretta gestione del trattamento dei flussi di dati raccolti attraverso il sito web*
- *Consulenza ai sensi del Provvedimento del Garante Privacy: Individuazione delle modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei cookie - 8 maggio 2014 (Pubblicato sulla Gazzetta Ufficiale n. 126 del 3 giugno 2014); Chiarimenti in merito all'attuazione della normativa in materia di cookie; Infografica 10 giugno 2015*
- *Predisposizione di apposita informativa estesa sui cookies sulla base dei Cookies da Voi utilizzati e a noi comunicati attraverso consulenza del vs. tecnico web, per*

inserimento sul Sito Web (Cookies policy)
- *Predisposizione di informativa breve (banner) sui cookies, ove necessario*
- *Istruzioni per vs. tecnico web circa modalità consenso e opt-in per invio cookies*

❖ ***Marketing e comunicazioni***
- *Verifica e aggiornamento dei Vs. documenti rispetto ai trattamenti da Voi effettuati in materia di Marketing, in riferimento alle Linee Guida del Garante privacy in relazione ad attività promozionali e contrasto allo Spam del 04 luglio 2013 (Gazzetta Ufficiale nr. 174 del 26/07/2013), e Provvedimento del Garante su consenso al trattamento dei dati personali per finalità di "marketing diretto" attraverso strumenti tradizionali e automatizzati di contatto - 15 maggio 2013 (Pubblicato sulla Gazzetta Ufficiale n. 174 del 26 luglio 2013) e successivi provvedimenti*
- *Consulenza su piattaforme in Cloud per servizio di invio newsletter e comunicazioni commerciali*

❖ ***Aggiornamento Normativo in materia di Privacy***
- *Invio delle informative relative agli aggiornamenti legislativi e a nuove misure adottate dal Garante Privacy*

❖ ***Consulenza Privacy***
- *Consulenza Privacy telefonica e/o e-mail al Referente Privacy o al DPO della Vs. struttura su eventuali richieste pervenute all'azienda in merito all'accesso ai dati degli interessati ed in generale per tematiche Privacy o data protection*

SERVIZIO RPD | DPO

Il Responsabile della protezione dei dati dovrà ottemperare a quanto previsto nel regolamento UE in epigrafe ed in dettaglio:

1. informare e consigliare il titolare o il responsabile del trattamento, nonché i dipendenti, in merito agli obblighi derivanti dal Regolamento europeo e da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati

2. verificare l'attuazione e l'applicazione del Regolamento, delle altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare o del responsabile del trattamento in materia di protezione dei dati personali, inclusi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale coinvolto nelle operazioni di trattamento, e gli audit relativi

3. fornire, se richiesto, pareri in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliare i relativi adempimenti

4. fungere da punto di contatto per gli interessati in merito a qualunque problematica connessa al trattamento dei loro dati o all'esercizio dei loro diritti

5. fungere da punto di contatto per il Garante per la protezione dei dati personali oppure, eventualmente, consultare il Garante di propria iniziativa

Modalità di svolgimento dell'attività:
1) sarà effettuato on site almeno un audit interno
2) verrà garantita la reperibilità tutti i giorni sabato e domenica compresi: telefonica dalle ore 9 alle ore 18, via mail 24/24, via Skype dalle 16 alle 18, verrà realizzato apposito gruppo WhatsApp per risposte istantanee. (in base alle modalità di contatto le risposte potranno essere istantanee e comunque al massimo entro le 24 ore, salvo che le stesse non richiedano un quesito al garante, nel qual caso la predisposizione del quesito è garantita entro 48 ore, la risposta seguirà i tempi del garante stesso)

PRESTAZIONI DEL COMMITTENTE

Al fine della buona riuscita dell'intervento consulenziale si rende necessario garantire, da parte del Committente, le seguenti attività:

- *La programmazione, il coordinamento degli incontri e dei sopralluoghi ivi compreso il rispetto del calendario degli stessi*
- *La presenza delle figure individuate in occasione delle riunioni e degli incontri programmati*
- *La sollecita fornitura della documentazione richiesta necessaria per avere un quadro preciso, esaustivo e completo dell'Azienda in termini sia organizzativi che tecnico/impiantistici*
- *Il pronto riscontro sulla documentazione predisposta ai fini della rapida revisione ed approvazione della stessa da parte delle funzioni preposte*
- *La corretta implementazione delle procedure e delle istruzioni messe a punto nonché la corretta registrazione delle attività svolte in accordo alla documentazione predisposta*
- *La tempestiva segnalazione di qualunque osservazione, dubbio o difficoltà riscontrati nell'implementazione del Sistema*

SANZIONI PRIVACY

L'art. 83 GDPR, rubricato "Condizioni generali per infliggere sanzioni amministrative pecuniarie", elenca i criteri che le singole Autorità di controllo dovranno applicare al momento di decidere se infliggere una sanzione amministrativa pecuniaria e di fissarne l'ammontare.

Lo stesso articolo individua due classi di violazioni:
Comma 4: fino a 10 MIL € o fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore per la violazione dei seguenti obblighi:

Gli obblighi del Titolare del trattamento e del Responsabile del trattamento a norma degli articoli 8, 11, da 25 a 39, 42 e 43 (es. violazione dell'obbligo di tenuta registro dei trattamenti, mancata valutazione di impatto DPIA; omessa consultazione preventiva Autorità di controllo, omessa notifica data breach).
Gli obblighi dell'organismo di certificazione a forma degli articoli 42 e 43.
Gli obblighi dell'organismo di controllo a norma dell'articolo 41, paragrafo 4.

Commi 5 e 6: fino a 20 MIL € o fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore per la violazione dei seguenti obblighi:

I principi di base del trattamento, comprese le condizioni relative al consenso, a norma degli articoli 5, 6, 7 e 9 (es. principi di liceità, correttezza e trasparenza, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità e riservatezza, diritto di revoca del consenso).
I diritti degli interessati a norma degli articoli da 12 a 22 (es. diritti di accesso, rettifica, cancellazione, portabilità dei dati, opposizione).
I trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale a norma degli articoli da 44 a 49.
Qualsiasi obbligo ai sensi delle legislazioni degli Stati membri adottate a norma del capo IX.
L'inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'autorità di controllo ai sensi dell'articolo 58, paragrafo 2, o il negato accesso in violazione dell'articolo 58, paragrafo 1. In merito alle altre sanzioni, tra cui le sanzioni penali, l'art 84 GDPR attribuisce delega agli Stati membri all'adozione di tutti i provvedimenti necessari per assicurarne l'applicazione. Sino a nuovi provvedimenti legislativi, restano in vigore le sanzioni penali previste dal Codice privacy (d.lgs. 196/03).

Il team di professionisti è costituito da:
Dott. Corrado Faletti, esperto di normativa e tecnologia
Avv Andrea Caristi esperto di Privacy e web identity
Roberto De Duro esperto di Cyber Security
Dott. Fabio Zafferri specialista in sistemi software
Rossella De Cosmo, analista funzionale

SI CONVIENE CHE

La convenzione proposta è così definita:

- **Per i Dirigenti Scolastici soci UDIR e/o che hanno stipulato una convenzione con Eurosofia** per la formazione del proprio personale scolastico:
  - Istituti secondari di secondo grado 700 euro iva esclusa
  - Istituti Comprensivi 500 euro iva esclusa

- **Per i Dirigenti Scolastici non soci UDIR o che non hanno stipulato una convenzione con Eurosofia** per la formazione del proprio personale scolastico:
  - Istituti secondari di secondo grado 1.500 euro iva esclusa
  - Istituti Comprensivi 1.000 euro iva esclusa

- **Per i Dirigenti Scolastici che attivano una rete di scuole (i costi sono riferiti ad una rete costituita da 5 scuole)**:
  - Istituti secondari di secondo grado 2.800 euro iva esclusa
  - Istituti Comprensivi 2.000 euro iva esclusa

Per qualunque altra esigenza specifica (ad esempio una rete di scuole costituita da più di 5 scuole oppure una rete costituita da istituti comprensivi e superiori) si rimanda alla stesura di un preventivo ad hoc e personalizzato in base alle richieste.

L'offerta prevede anche l'eventuale trasformazione del contratto in caso di diverse disposizioni di legge per le scuole, in corsi di formazione dedicati da erogare tramite EUROSOFIA, ente accreditato MIUR ai sensi della direttiva 170/2016.

Letto, approvato e sottoscritto in _____il_____

Legale Rappresentante

Il Dirigente Scolastico

ALLEGATO A

ADESIONE AL PROTOCOLLO DI INTESA

Cognome		Nome	
Data di nascita		Luogo di nascita	
Codice fiscale		Email	
Cellulare		Altro recapito telefonico	
In qualità di DIRIGENTE SCOLASTICO dell'Istituto			
Indirizzo			
Codice meccanografico della scuola			
Convenzione per soci Udir e/o che hanno stipulato una convenzione con Eurosofia	Istituti secondari di secondo grado € 700,00 ☐ Istituti comprensivi € 500,00 ☐		
Convenzione per non soci Udir o che non hanno stipulato una convenzione con Eurosofia	Istituti secondari di secondo grado € 1.500,00 ☐ Istituti comprensivi € 1.000,00 ☐		
Convenzione per una rete di scuole	Istituti secondari di secondo grado € 2.800,00 ☐ Istituti comprensivi € 2.000,00 ☐		

Indicare con una "X" la convenzione prescelta

AUTORIZZAZIONE AL TRATTAMENTO DEI DATI PERSONALI
(INFORMATIVA AI SENSI DEGLI ARTT. 13 E 14 DEL GDPR – REGOLAMENTO UE/2016/679)

Con la presente il/la sottoscritto/a_____

DICHIARA

- di essere stato informato, ai sensi degli artt. 13 e 14 del GDPR -UE/2016/679 sulla tutela dei dati personali, che i propri dati personali forniti all'atto della compilazione della presente richiesta saranno trattati in conformità alle norme legislative e regolamentari vigenti e applicabili, con modalità automatiche, anche mediante sistemi informatizzati solo ed esclusivamente nell'ambito delle operazioni necessarie a consentire il corretto svolgimento e funzionamento di tutte le attività legate alle attività proposte;
- di acconsentire con la presente dichiarazione, al trattamento dei propri dati personali, svolto con le modalità e per le finalità sopra indicate, ed in conformità alle norme legislative e regolamentari vigenti e applicabili;

- di essere a conoscenza che titolare del procedimento è Eurosofia

Luogo e data, lì _____

(Firma)

Per accettazione

_____