EDU Consulting srl
Via XX Settembre, 118
00187 Roma
tel. 06 8715323
www.educonsulting.it - gdpr@educonsulting.it
Ufficio di Caserta: 0823753477

partner Asso Edu
Associazione Nazionale Tecnologie e Digital Media per l'Educazione

All'attenzione del Dirigente Scolastico

Oggetto:	**Offerta relativa al rinnovo per la consulenza, l'adeguamento e la redazione documentale relativa all'attuazione del Regolamento Europeo N. 679/16 - *GDPR (General Data Protection Regulation)*.**

EDU Consulting srl
Via XX Settembre, 118
00187 Roma
tel. 06 8715323
www.educonsulting.it - gdpr@educonsulting.it
Ufficio di Caserta: 0823753477

partner Asso Edu
Associazione Nazionale Tecnologie e Digital Media per l'Educazione

Dettagli dell'offerta Sistema di Gestione Privacy

Sommario

1. PREMESSA

Il nuovo regolamento Europeo (GDPR) ha imposto nuovi standard di riferimento a tutte le Aziende/Enti/PA che trattano DATI personali, sensibili e giudiziari.
La consulenza sul tema privacy comprende una serie di attività volte a valutare l'acquisizione, il trattamento e la conservazione dei dati, migliorandone l'efficacia e garantendone il completo rispetto dell'attuale normativa.
Per svolgere efficacemente tale compito, la nostra società ha definito una serie di attività atte a risolvere in modo organico il tema, affiancando il cliente nell'opera di adeguamento, mantenimento dei processi e della relativa gestione documentale, e soprattutto idonea ad offrire strumenti di controllo e di monitoraggio indispensabili per la gestione nel tempo della sicurezza e del parco IT.

1.1 PRINCIPALI NOVITÀ INTRODOTTE DAL GDPR

La maggior incidenza ed impegno si avrà nell'Area organizzativa. Il regolamento è costruito sul principio della responsabilizzazione (accountability) di titolari e responsabili del trattamento, il che si traduce in una serie di comportamenti proattivi da parte di chi tratta dati personali. L'intervento delle autorità di protezione dati è soprattutto ex post, non ex ante; non ci sono più obblighi di notifica preventiva o autorizzazione preventiva da parte dell'autorità. Il bilanciamento di interessi (rispetto all'interesse legittimo del titolare) spetta al titolare stesso, assistito da linee-guida delle autorità europee, ma che opera autonomamente".

1.2 REGISTRO ATTIVITÀ

Con il Regolamento UE 2016/679 il titolare deve tenere un registro delle attività svolte sotto la propria responsabilità. Tale registro, su richiesta, deve essere messo a disposizione dell'Autorità di controllo. In questo registro, fra le altre informazioni, devono essere riportate le misure di sicurezza tecniche ed organizzative adottate.
<u>Valutazione d'impatto sulla protezione dei dati:</u>
Il titolare prima di procedere con il trattamento è tenuto ad effettuare una valutazione di impatto; sulla medesima dovranno essere evidenziati anche i rischi e le misure previste per

affrontarli, descrivendo le misure di sicurezza adottate per proteggere i diritti e gli interessi legittimi degli interessati.

1.3 ACCOUNTABILITY

Il principio dell'accountability richiede che il titolare del trattamento metta in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al GDPR. Per raggiungere tale obiettivo, misurato sulla valutazione del rischio, occorre dotarsi di infrastrutture che possano sostenere l'Onere della Prova.

1.4 CODICI DI CONDOTTA E CERTIFICAZIONE

Un'importante novità del Regolamento è la previsione di meccanismi di certificazione, sigilli e marchi di protezione dei dati che consentano agli interessati di valutare rapidamente il livello di protezione dei dati dei relativi prodotti e servizi.
L'adesione ai codici di condotta e la certificazione del trattamento sono elementi di cui l'Autorità dovrà tenere conto, per esempio, nell'applicare eventuali sanzioni o nell'analizzare la correttezza di una valutazione di impatto effettuata dal titolare del trattamento.

1.5 PRIVACY BY DEFAULT & BY DESIGN

Con la terminologia by default e by design si intende indicare la tutela dei dati personali determinata come impostazione predefinita (by default) e pensata fin dalla progettazione di servizi, tipo quelli scolastici (by design). L'intento è quello di prevenire e non correggere. L'obiettivo è la sintesi del "By-Default + By-Design", cioè consentire all'utente l'attività del trattamento del DATO in assoluta tranquillità, in modalità "*Compliance*" con il Regolamento GDPR, escludendo a priori, trattamenti non coerenti dei DATI.

1.6 MISURE IDONEE

Le novità introdotte dal GDPR, con riferimento all'analisi del rischio digitale, sono moltissime.
A seconda della tipologia di attività e trattamento effettuati dall'Organizzazione, il Titolare ha l'obbligo di individuare adeguate misure di sicurezza relative ai dati personali da essa trattati.
Si passa dalle vecchie – ormai superate - misure minime di sicurezza (ES: complessità password di almeno 8 caratteri con scadenza ogni 3 mesi se si tratta di dati sensibili.) alle attuali misure idonee.
Quest'ultime non le troviamo elencate in nessuna norma o allegato, poiché cambiano a seconda dello «scenario digitale» in cui il dato «vive».
Misure idonee di sicurezza sono da intendere come la metodologia improntata sul livello di sicurezza adeguata al rischio, da analizzare, implementare, ma soprattutto, da verificare periodicamente.

2. GDPR PUNTI DI ATTENZIONE

2.1 QUALI SONO I DATI PERSONALI ?

Secondo la Commissione Europea "i dati personali sono qualunque informazione relativa ad un individuo, collegata alla sua vita sia privata, sia professionale che pubblica. Può riguardare qualunque cosa: nomi, foto, indirizzi email, dettagli bancari, interventi su siti web di social network, informazioni mediche o indirizzi IP di computer."

2.2 PERCHE PREOCCUPARSENE ?

Esiste un vincolo di obbligatorietà per tutte le aziende che trattano DATI personali. Oltre a tale obbligo vi sono una serie di sanzioni che nascono dall'aver equiparato il trattamento dei DATI personali ad una attività di tipo pericolosa. Le sanzioni per la non conformità sono enormi e dipendono dall'infrazione.

2.3 I DIRITTI DELL'INTERESSATO

- Notifica delle violazioni
- Diritto di accesso ai dati
- Diritto all'oblio
- Portabilità dei Dati
- Privacy by Design

2.4 LE FIGURE INTERESSATE

Il Titolare del Trattamento, ora chiamato Data Controller o Responsabile del trattamento, è dotato di un potere decisionale in ordine alle tecniche da adottare ed alle misure organizzative, al fine di garantire la conformità al Regolamento delle operazioni di trattamento dei dati.
Il Responsabile esterno del Trattamento / Amministratore di Sistema, ora chiamato Joint Controller o Co-responsabile del trattamento anche in outsourcing.
Il responsabile ed incaricato del trattamento, ora chiamato Data Processor e Incaricato del Trattamento o più semplicemente Data Handler, sarà l'attuale responsabile e potrà procedere al trattamento dei dati solo su istruzione del responsabile.
Il responsabile della sicurezza dei dati, ora chiamato Data Protection Officer (DPO) meglio descritto nel seguito.

2.5 DATA PROTECTION OFFICERS

E' un'interfaccia di riferimento preposta nei rapporti con il Garante stesso, non deve rivestire particolari responsabilità nella gestione del trattamento dei dati.
Obbligatorio in questi casi:

- Amministrazioni ed enti pubblici, fatta eccezione per le autorità giudiziari;
- Tutti i soggetti la cui attività principale consiste in trattamenti che, per la loro natura, il loro oggetto o le loro finalità, richiedono il controllo regolare e sistematico degli interessati;
- Tutti i soggetti la cui attività principale consiste nel trattamento, su larga scala, di dati sensibili, relativi alla salute o alla vita sessuale, genetici, giudiziari e biometrici.

Deve essere nominato in base alla qualità professionali:

- Può essere un membro del personale o un fornitore di servizi esterno
- Riporta direttamente al più alto livello manageriale
- Non deve svolgere eventuali ulteriori compiti.
- Può essere una figura esterna alla scuola.

3. I SERVIZI OFFERTI

Occorre garantire il più possibile la serenità alle scuole, passando attraverso la consapevolezza che ogni attività svolta sulla rete informatica deve diventare controllabile, verificabile e quindi registrabile (ad esempio tecnicamente: Log di Accesso ai sistemi, alla navigazione Web, per la copia o spostamento di documenti).
La nostra consulenza sarà sia di tipo legale che di tipo tecnico: La scelta della tecnologia non è più facoltativa, ma diventa propedeutica a tale vincolo e pertanto occorre porre molta attenzione

e scrupolosità nell'analisi degli attuali sistemi informatici e nella scelta di quelli futuri (Privacy by Design). L'attenta valutazione d'impatto e di rischio, permetterà all'Organizzazione di individuare potenziali rischi e adottare adeguate misure sin dai primi processi di progettazione ed implementazione dei sistemi.
Il nostro obiettivo è quello di creare un sistema sicuro "by design" e "by Default", dove l'operatore può svolgere le sue attività in tranquillità perché il sistema è in grado di farlo lavorare in modo sicuro e conforme alle normative.
Il servizio prevede lo svolgimento dei compiti definiti dal GDPR da parte della persona fisica designata come DPO.
Durata dell'incarico: un anno dalla data di perfezionamento dell'incarico
Rinnovo: a seguito di un nuovo accordo.
Il servizio proposto include, a titolo di esempio:

- Sopralluogo e Audit generali suddivisi (a titolo di esempio):

Primo Audit	Secondo Audit	Terzo Audit
Audit essenzialmente tecnico: è prevista l'analisi della rete, dei computer degli uffici e del sito Web.	Audit documentale: analisi delle conformità documentali e valutazione delle attività svolte. Formazione personale Amministrativo ed incaricati.	Audit finale: Valutazione delle buone pratiche applicate. Programmazione interventi da correggere e/o integrare.

- Predisposizione e supporto alla redazione della modulistica personalizzata (nomine, registro dei trattamento, valutazione d'impatto, ecc.).
- Fornitura di modelli e buone pratiche per l'applicazione della normativa in materia di privacy, trasparenza, accessibilità, digitalizzazione e lotta alla corruzione incluse linee guida, regolamento necessarie a formalizzare gli incarichi previsti dalla normativa;
- Eventuale redazione della valutazione d'impatto (Data Protection Impact Assessment, "DPIA")
- Accesso riservato ad un apposito spazio web, aggiornato, contenente una sintesi dei principali adempimenti derivanti dalla normativa vigente in materia di privacy, trasparenza, lotta alla corruzione, digitalizzazione (bozze dei documenti da produrre, fogli di calcolo, ecc.).
- Piano di formazione sarà finalizzata alla preparazione del personale incaricato, sempre in materia di protezione dei dati e privacy, riguardo le operazioni da eseguire. Si prevedono circa tre ore per il personale di segreteria e collaboratori scolastici (modalità *onsite*), ed altre n. 3 ore per i docenti (anche con uso di piattaforma FAD). Si possono prevedere sedute aggiuntive ogni volta che lo si ritenga necessario: è indispensabile rendere autonomo il personale stesso nello svolgimento del compito assegnato. La formazione sarà effettuata in presenza e si metterà a disposizione una piattaforma E-Learning con webinair tematici disponibili.

In sintesi:

A. **Designazione DPO per anno solare;**
B. **Attività ed adempimenti relativi alla nomina di DPO compresivi max di n. 3 interventi della durata massima di una giornata cad. per ogni anno solare;**
C. **Preparazione della documentazione completa richiesta;**
D. **Consulenza telefonica e documentale giornaliera;**
E. **Formazione: interventi di formazione per incaricati (3 ore onsite), utilizzo di piattaforma FAD dedicata con generazione di attestazione per tutti i dipendenti;**
F. **Piattaforma documentale per gestire / generare ed utilizzare i documenti direttamente con l'intestazione della scuola;**

4. OFFERTA ECONOMICA

Offerta Economica per la Realizzazione del Sistema di Gestione Privacy per la conformità al Regolamento UE 679/2016 (GDPR), l'offerta comprende:

- L'auditing presso la sede della scuola
- Il censimento, la raccolta dati e la verifica della conformità alla normativa
- La stesura informative personalizzate e consensi
- La gestione degli atti di nomina
- Il data mapping (organigramma)
- Privacy by design ed il registro dei trattamenti
- L'analisi dei rischi
- Il DPIA - Data Protection Impact Assessment -Risk Assessment
- Il Workflow e la gestione del DPO - Data Protection Officer
- Gestione del Data Breach
- La redazione e consegna del report finale in forma cartacea
- Realizzazione GDPR con l'ausilio di del DPO

Costi previsti

Servizio proposto	*Importo Annuo*	*Totale importo*
A. Contratto per una sola annualità	€ **1.129,00** + iva	€ **1.129,00** + iva

Eventuali interventi opzionali aggiuntivi su richiesta del Titolare sono da concordare

Tempi di Realizzazione:

Le attività saranno svolte in data da concordare, e comunque con l'ausilio di Vs. personale, nello specifico con le persone da voi nominate alla gestione del trattamento.

Condizioni generali di fornitura:

- I prezzi si intendono al netto di IVA 22%
- Pagamento: 50% al contratto e altro 50% al termine del servizio
- Intervento fruito: Chiavi in mano

l'ausilio di Vs. personale, nello specifico con le persone da voi nominate alla gestione del trattamento. I nostri numeri di riferimento sono i seguenti:

EDU Consulting srl
Via XX Settembre, 118 - 00187 Roma
www.educonsulting.it - gdpr@educonsulting.it
Ufficio di Roma: 06 8715323 - Ufficio di Caserta: 0823.753477

L'Amministratore