

**Proposta di Collaborazione per adempimenti**

**sul Trattamento dei Dati Personali ai sensi**

**del Regolamento UE 679/2016**

**in Compliance alla Norma ISO/IEC 27001:2017** **e nel rispetto**

**del D. Lgs. 24/2023 in tema di Whistleblowing**

**Rev. 01 del 07/10/2024**

Proposta per:

**SOTRAS S.R.L.**

**c.a.**

**ISABELLA RUZZA**

**Spett.le**

**SOTRAS S.R.L.**

**c.a.**

**ISABELLA RUZZA**

Settimo T.se, 07/10/2024

Ns. Rif. (Protocollo ns interno)

|  |  |
| --- | --- |
| **Oggetto:** | **Proposta di Collaborazione per Consulenza sulla Protezione delle Persone Fisiche, con riguardo al Trattamento dei Dati Personali di cui al Regolamento Europeo 2016/679, in Compliance alla Norma ISO/IEC 27001:2017 e nel rispetto del D. Lgs. 24/2023 in tema di Whistleblowing.** |

Con la presente siamo lieti di mettere a Vs. disposizione le ns. competenze per la transizione agli adempimenti connessi al Regolamento Europeo 679 del 27 Aprile 2016 (GDPR – Regolamento Generale della Protezione dei Dati) in Compliance alla Norma ISO/IEC 27001:2017, per le Organizzazioni (SOTRAS S.R.L.).

Ove applicabile Vi comunichiamo che in ottemperanza agli obblighi in materia di segnalazione di illeciti “Whistleblowing” di cui al D. Lgs. 24/2023, la ns Organizzazione effettuerà un’analisi preliminare al fine di verificare se la vs realtà è soggetta o meno agli adempimenti. In caso di esito positivo provvederemo a redigere tutta la documentazione necessaria a raggiungere la conformità.

Gruppo CS è una società specializzata in consulenza privacy e nell’implementazione di sistemi di gestione, in grado di affiancare la Vs. Organizzazione e supportarla in tutte le fasi del percorso di adeguamento alle norme cogenti.

Al fine di comprendere in modo puntuale gli adempimenti da sottintendere, che vi consentiranno di raggiungere la Conformità Legislativa, riteniamo necessario elencarli di seguito, nel dettaglio le disposizioni del GDPR integrate alla Norma ISO/IEC 27001:2017.

Per ognuno dei sottoindicati punti, i Consulenti di Gruppo CS saranno in grado di valutare l’attuale stato di compliance della vs. Organizzazione, pianificando il percorso più adeguato a adempiere ai seguenti obblighi previsti dal Regolamento Europeo Privacy:

* Adeguamento della Vs. Organizzazione ai Principi Generali del Regolamento Privacy 2016/679 UE;
* Ridefinizione dell’organigramma Privacy aziendale;
* Individuazione e nomina dei soggetti incaricati al Trattamento dei Dati Personali, interni ed esterni;
* Riclassificazione dei Dati Personali e dei relativi Trattamenti;
* Verifica dei nuovi Trattamenti effettuati e chiusura dei precedenti;
* Adempimento degli obblighi privacy in materia di Profilazione (art.21 e 22);
* Valutazione d'impatto sulla protezione dei dati trattati (art.35);
* Valutazione e Tutela dei Rischi;
* Definizione delle misure minime di sicurezza;
* Adozione di Codici di Condotta Privacy;
* Procedure Interne e Data Breach;
* Rispetto dei requisiti della "Privacy by Design" e "Privacy by Default";
* Definizione degli adempimenti connessi alla Formazione del Personale;
* Gestione dei Sistemi di Videosorveglianza (ove previsto);
* Adempimenti Linee Guida su Cookies e altri strumenti di tracciamento;
* Adeguamento Privacy Policy Sito Web Aziendale;
* Adempimenti formativi del personale interno (Referente e Autorizzati);
* Definizione della struttura informatica, del sistema informativo e delle relative caratteristiche;
* Ove applicabile, redazione nomina Responsabile Gestione del Canale Interno di Segnalazione;
* Ove applicabile, istituzione del Canale Interno di Segnalazione di Illeciti;
* Ove applicabile, redazione della Whistleblowing Policy.

Per quanto concerne la ISO/IEC 27001:2017 gli elementi presenti nella Norma che saranno integrati all’interno della documentazione privacy sono i seguenti:

* ***Definizione del Contesto dell’organizzazione***

Paragrafo 4.2 Comprendere le necessità e le aspettative delle parti interessate definendo il perimetro di azione dei trattamenti dati effettuati e i requisiti di sicurezza da implementare.

* ***Leadership***

Paragrafo 5.2 Redigere e mettere a disposizione degli Stakeholder la Politica della sicurezza delle informazioni.

Paragrafo 5.3 Ruoli, responsabilità e autorità nell’organizzazione saranno presenti nel nuovo organigramma privacy.

* ***Pianificazione***

Paragrafo 6.1.2. Valutare il rischio relativo alla sicurezza delle informazioni.

Paragrafo 6.1.3. Comparazione dei controlli utilizzati per la sicurezza delle informazioni con quelli presenti nell’Annex A della Norma.

* ***Supporto***

Paragrafo 7.1 – 7.2 – 7.3 Soddisfare i requisiti richiesti della competenza e della consapevolezza attraverso la pianificazione dei percorsi formativi per il personale interno.

* ***Valutazione delle prestazioni***

Paragrafo 9 Monitoraggio, misurazione, analisi e valutazione. Attività incluse all’interno dell’Auditing periodico sul sistema di gestione privacy.

* ***Miglioramento***

Paragrafo 10 Definizione di un piano di intervento annuale sul mantenimento e sull’aggiornamento del sistema di gestione.

*Ci pare importante evidenziare che ai fini di una futura Certificazione del Sistema di Gestione del Trattamento Dati, in conformità alla ISO/IEC 27001:2017, si renderà necessario l’implementazione di TUTTI I PUNTI RESTANTI; previsti dalla norma indicata.*

Per tutti gli adempimenti GDPR sopra descritti, verrà prodotta una evidenza documentale, attraverso:

* La Redazione del Manuale del Sistema di Gestione Privacy, compliance alla ISO/IEC 27001:2017;
* L’ approntamento delle nomine delle figure coinvolte (Responsabili Esterni, Persone autorizzate al Trattamento Dati, Referente Interno del Trattamento Dati…);
* La redazione delle Informative Privacy e Consenso al Trattamento;
* La predisposizione della Nomina del Responsabile della Protezione dei Dati (ove presente);
* La redazione di modelli "Master" per disciplinare i rapporti di contitolarità, compliance alla ISO/IEC 27001:2017;
* La regolamentazione del Codice di Condotta Interno / di Settore.

***DELIVERABLES DI PROGETTO***

L'obiettivo del progetto è l’assistenza nella realizzazione di tutti gli adempimenti atti a verificare e soddisfare, all’interno della Vs. azienda, l’applicazione di tutti i requisiti cogenti previsti dal Regolamento Europeo 2016/679.

Confermiamo altresì che tutti gli elementi previsti dal progetto garantiranno alla Vs. organizzazione la piena compliance alla Norma ISO/IEC 27001:2017 ma che gli stessi non saranno esaustivi per affrontare un eventuale iter certificativo.

Ove soggetti al D. Lgs. 24/2023, forniremo le evidenze documentali e procedurali necessarie al rispetto della normativa nazione in materia di segnalazione di illeciti.

L’intervento consulenziale è finalizzato all’ottenimento del massimo vantaggio aziendale, derivato e collegato al lavoro di analisi effettuato, per migliorare le procedure, distribuire le responsabilità, coinvolgere tutti i soggetti dell’Azienda in una seria politica di sicurezza del trattamento dei dati.

Gruppo CS, pertanto, supporta l’azienda nell’assolvimento di una cogenza normativa, che nonostante l’investimento economico diventa un’opportunità di business e di tutela verso il mercato economico sempre più digitale e concorrenziale.

Il personale tecnico coinvolto comprende esperti dell’ambito Privacy (normata in precedenza dal D.Lgs. 196/03 e prima ancora dal D. Lgs. 675/96), Avvocati competenti in materia giuridica, Esperti Informatici e Consulenti su sistemi di gestione.

***PROGRAMMA DELLE ATTIVITA’***

Il programma delle attività prevede un Intervento di «Assistenza Complessiva» nel quale vengono garantiti, in una proposta a corpo, gli interventi di adeguamento necessari.

Tale Proposta di Assistenza è finalizzata a supportarvi nel Processo di Gestione e Monitoraggio degli Adempimenti Privacy di cui al Regolamento UE 679/2016 in conformità alla Norma ISO/IEC 27001, attraverso:

1. **Una prima attività di raccolta dati**, a cura dei nostri tecnici presso la vostra sede per svolgere:
* l’analisi della struttura aziendale, il personale interno ed esterno coinvolto, i trattamenti (informatici e cartacei) dei dati effettuati;
* la valutazione di impatto sulla protezione dei dati;
* la valutazione dei rischi e le procedure di tutela da attivare;
* la verifica degli strumenti web utilizzati (sito web, social network, servizi web);
* l’individuazione delle procedure interne;
* l’analisi delle politiche di creazione e gestione di Banche Dati (Privacy by Design e Privacy by Default);
* l’individuazione delle figure operative e responsabili sul Sistema di Gestione privacy, inclusi i relativi requisiti formativi cogenti;
* la raccolta documentale necessaria a supportare la redazione dei documenti privacy.

Per dette attività, sono previste xx giornate lavorative in presenza presso la vs sede, pari a 4 h. per ogni organizzazione oggetto della presente proposta (TEATRO GIOCO VITA SRL).

1. **È prevista una seconda attività,** presso la vs. sede, della durata di circa 8h, con la collaborazione e supporto dei tecnici della Vs. Area IT, al fine di effettuare, in modo accentrato per le xx Società:
* la verifica degli strumenti informatici utilizzati (hardware lato client e lato server, software operativi, gestionali, applicativi, sistemi di protezione, cyber security, sistemi di salvataggio e ripristino nonché tutte le caratteristiche del sistema informativo dell’azienda).
1. **Una terza attività di elaborazione dati**, svolta presso la sede di Gruppo CS, a cura dei nostri tecnici per:
* la rielaborazione del materiale raccolto,
* la predisposizione dell’Impianto Documentale Privacy,
* la redazione delle nomine per gli incaricati, interni ed esterni, e dei relativi responsabili;
* la revisione del vs. Codice di Condotta Aziendale, ovvero l’azione di un Codice di Condotta di Settore;
* la stesura della documentazione cogente previste e delle eventuali procedure operative interne;
* La produzione di una matrice che individui le relazioni con i requisiti previsti dalla Norma ISO/IEC 27001 (Presenti e/o Mancanti).
1. **Una quarta attività di condivisione**, da svolgere presso la vostra sede, nella quale verrà realizzata:
* la condivisione e consegna del materiale prodotto (Manuale Privacy in formato cartaceo, nomine e codici in formato elettronico);
* l’analisi degli adempimenti previsti e delle modalità di utilizzo del materiale predisposto;
* il supporto nella resa operativa e funzionale del Sistema di Gestione Privacy;
* un riscontro operativo sui punti implementati, afferenti ai requisiti della Norma ISO/IEC 27001.

Per tali attività sono previsti xxx incontri separati, di circa 02 h. ciascuno, in presenza presso la vs. sede, dedicati alle organizzazioni oggetto della presente proposta (TEATRO GIOCO VITA SRL) per la durata complessiva di una giornata.

***INVESTIMENTO ECONOMICO DEL PROGRAMMA***

Intervento di «Assistenza Complessiva»:

Costo totale offerta ***Euro 600 + Iva***

Costo a Voi riservato ***Euro 600 + Iva***

***Il costo è comprensivo della redazione di tutti i documenti previsti nel punto «Programma delle Attività», nonché degli incontri e trasferte previsti presso vostra sede.***

La presente offerta ha una validità di 30 giorni a decorrere dalla data odierna.

**Formalizzazione incarico:**

GRUPPO CS formalizza l'accordo con la Vs. Azienda attraverso la firma del presente incarico.

**Rapporti operativi:**

GRUPPO CS illustrerà, al termine del progetto, quanto realizzato e indicherà le attività da svolgere a carico del Cliente.

**Fatturazione:**

GRUPPO CS gestirà la fatturazione come segue:

***Per Presa Visione ed Accettazione (timbro e firma)***

***\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_***

***(Luogo e Data)***

***\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_***

***REGOLAMENTO EUROPEO 679/2016***

In conformità a quanto previsto nel Regolamento Europeo 679/2016, ai sensi dell’art. 13, è nostro dovere informarVi che i Vs. dati personali saranno trattati esclusivamente per le finalità riportate di seguito:

a) dirette esclusivamente all’assolvimento degli obblighi contrattuali o per l’acquisizione di informative precontrattuali, nonché per informazioni relative a richieste dell’interessato di forniture e servizi.

b) connesse agli obblighi previsti da leggi, da regolamenti e dalla normativa comunitaria nonché da disposizioni impartite da autorità a ciò legittimate e da organi di vigilanza e controllo, nonché agli obblighi in materia fiscale e contabile;

c) per attività di comunicazione, anche di natura commerciale.

ll trattamento dei dati personali avviene mediante strumenti manuali, informatici e telematici con logiche strettamente correlate alle finalità stesse e, comunque, in modo da garantire la sicurezza e la riservatezza dei dati stessi nonché conservati in una forma che consenta la sua identificazione per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati.

I dati raccolti rientrano nella categoria dei dati personali identificativi di contatto strettamente connessi e strumentali alla gestione dell’attività di consulenza.

Vi rendiamo conto che l’art. 15 del Regolamento Europeo, il cui testo è disponibile presso gli uffici del Gruppo CS, conferisce all’interessato il potere di esercitare specifici diritti a propria tutela.

Inoltre, Vi segnaliamo che tutto il personale del GRUPPO CS sottoscrive un impegno di riservatezza rispetto alle informazioni e ai dati acquisiti nel corso dell’attività professionale presso i Clienti.

***Per Presa Visione ed Accettazione***

***\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_***

***CONTATTI E RIFERIMENTI:***

***CONTATTI E RIFERIMENTI:***

Per ogni eventuale chiarimento, la ns. sede direzionale di Torino,

è a Vs. completa disposizione ai seguenti recapiti:

**Gruppo CS - Via Leinì 23 - 10036 Settimo T.se – TO**

**Telefono: 011 - 897.00.64**

**Web site:** www.gruppocs.com **Mail:** info@gruppocs.com

Persona di Contatto: Turi Felipe Aramu

**Telefono: 011 - 897.24.00 interno 711 Mail:** privacy@gruppocs.com

****

**Filiale di Alessandria:**Piazza S.Maria di Castello,14 - 15100 Alessandria
**Filiale di Milano:**Via Cornalia, 19 - 20124 Milano
**Filiale di Varese:**
Via Guanella, 43 - 21027 Barza d'Ispra - VA
**Filiale di Bratislava:**Gorkèho, 3 - 811 01 Bratislava  - Slovacchia