

**Proposta di Collaborazione per Monitoraggio e Controllo Periodico sul Sistema di Gestione per il**

**Trattamento dei Dati Personali**

**ai sensi del Regolamento UE 679/2016 in Compliance alla Norma ISO/IEC 27001:2017**

**Rev. 01 del gg/mm/aaaa**

Proposta per:

**BANCO FARMACEUTICO TORINO ODV**

**VIA BRUNETTA 11, TORINO, Torino, 10139, Italia**

**Spett.le**

**BANCO FARMACEUTICO TORINO ODV**

**c.a.**

**(Nome e Cognome)**

Settimo T.se, gg mm aaaa

Ns. Rif. \_\_\_\_\_/24/RC/at

|  |  |
| --- | --- |
| **Oggetto:** | **Proposta di Collaborazione per Monitoraggio e Controllo Periodico sul Sistema di Gestione per il Trattamento dei Dati Personali di cui al Regolamento Europeo 2016/679 ed in Compliance alla Norma ISO/IEC 27001:2017.** |

Siamo lieti di mettere a Vs. disposizione le ns. competenze, per il monitoraggio e controllo periodico sul Sistema di Gestione Privacy, realizzato in Compliance al Regolamento Europeo 679/2016 e alla Norma ISO/IEC 27001:2017, delle Organizzazioni (BANCO FARMACEUTICO TORINO ODV), così come previsto dall’art. 24 del GDPR il quale specifica che il “*titolare del trattamento mette in atto misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate”.*

Tale principio è ribadito dall’art. 39 comma 1 lettera b) del Regolamento Europeo 679/2016 il quale stabilisce che uno dei compiti fondamentali del Responsabile Privacy è «*sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo».*

Gruppo CS, in quanto società specializzata nei Sistemi di Gestione ivi compresa la consulenza in ambito Privacy, è in grado di affiancare le Vs. Organizzazioni al fine di rispondere a quanto richiesto dal Regolamento Europeo in merito ad una sorveglianza periodica e costante del Sistema di Gestione aziendale.

***DELIVERABLES DI PROGETTO***

L'obiettivo del progetto è l’applicazione di quanto richiesto dagli articoli 24 e 39-1b) del Regolamento citato, in ottica di garantire un costante monitoraggio della messa in atto delle politiche adottate dal titolare e/o referente interno del trattamento dei dati in ambito di protezione dei dati personali, in particolare:

* Verifica delle responsabilità attribuite al personale interno ed esterno all’azienda, nel rispetto del trattamento dei dati;
* Verifica del sistema di protezione dati adottato e del suo funzionamento;
* Verifica della avvenuta formazione del personale.

L’intervento consulenziale è finalizzato inoltre alla revisione e controllo dell’intero sistema di gestione Privacy secondo le disposizioni del Regolamento Europeo, in Compliance alla Norma ISO/IEC 27001:2017.

***PROGRAMMA DELLE ATTIVITA’***

Il programma delle attività prevede una serie di interventi orientati al «Metodo di Controllo» nel quale vengono garantiti, in una proposta a corpo, tutti gli interventi di monitoraggio del Sistema di Gestione Privacy, compliance al Regolamento Europeo e alla Norma ISO/IEC 27001:2017.

Di seguito si riporta l’elenco dettagliato delle attività previste:

* Un audit semestrale di autovalutazione aziendale effettuato per ogni organizzazione oggetto del contratto (BANCO FARMACEUTICO TORINO ODV), disponibile su nostra piattaforma informatica di Assessment (redazione a cura del Cliente), al termine del quale saranno prodotti da Gruppo CS quattro specifici report, orientati a produrre le evidenze del monitoraggio cogente, nonché il riscontro di quanto indicato nel Vs. Manuale Privacy;
* Un audit, con cadenza annuale per ognuna delle 4 aziende indicate, presso la vostra sede o in alternativa, a vs. scelta, in modalità a distanza (da remoto), al fine di aggiornare i Manuali Privacy. L’Audit verrà pianificato sulla base delle seguenti caratteristiche da verificare:

**A.1 Politica e obbligazioni del Titolare**

A1.1 – Obblighi generali e consapevolezza del Titolare

Obiettivo: Stabilire la corretta percezione e applicazione formale del concetto di responsabilità generale del Titolare del trattamento

A1.2 – Misure tecniche e organizzative per la protezione dei dati personali

Obiettivo: Stabilire se il Titolare ha adottato tutte le politiche interne per garantire l’applicazione dei principi di protezione dei dati personali

A1.3 – Valutazione di Impatto sui diritti e sulle libertà dei soggetti interessati derivanti dalla possibile perdita di sicurezza dei dati

Obiettivo: Potenziare il rispetto del regolamento per trattamenti che possono presentare rischi elevati circa i diritti e le libertà fondamentali delle persone fisiche

A1.4 – Valutazione dei Rischi di trattamento

Obiettivo: Classificazione e Valutazione preventiva dei rischi connessi alle diverse aree di trattamento

A1.5 – Revisione e aggiornamento dei Registri di trattamento

Obiettivo: Classificare i nuovi trattamenti dati, nominare i soggetti interni/esterni autorizzati al trattamento, definire su quali basi giuridiche si fonda il trattamento

**A.2 Soggetti che effettuano il trattamento**

A2.1 Titolare del trattamento

Obiettivo: Assicurare il rispetto delle norme vigenti da parte del Titolare

A2.2 Referente Interno del trattamento

Obiettivo: Assicurare il rispetto delle prescrizioni del Titolare e assolvere gli adempimenti formativi

A2.3 Autorizzati al trattamento

Obiettivo: Assicurare il rispetto delle disposizioni di legge in materia di trattamento dei dati e adempiere agli obblighi formativi

A2.4 Responsabili Esterni

Obiettivo: Assicurare il rispetto delle indicazioni del Titolare fornite mediante lettera di nomina

A2.5 Amministratore di Sistema

Obiettivo: Assicurare la corretta gestione del sistema informativo in funzione dei rischi di trattamenti dati rilevati

**A.3 Principi del Trattamento**

A3.1 Responsabilizzazione (Accountability)

Obiettivo: Assicurare la corretta applicazione dei principi di trattamento e di qualità dei dati

A3.2 Sicurezza del trattamento

Obiettivo: Assicurare la gestione in sicurezza dei dati personali

A3.3 Principi di volontarietà del trattamento dei propri dati personali – Consenso

Obiettivo: Valutare l’esatta consapevolezza dell’interessato nel manifestare il suo consenso al trattamento

A3.4 Informativa sul trattamento dei dati personali

Obiettivo: Valutare la corretta procedura di rilascio dell’informativa all’interessato, aggiornare i termini secondo le indicazioni fornite dal Garante e dalle Autorità Europee

A3.5 Diritti dell’interessato

Obiettivo: Valutare il corretto rispetto dell’esercizio dei diritti dell’interessato

A3.6 Attività di profilazione

Obiettivo: Assicurare una corretta gestione della profilazione

Per quanto concerne la ISO/IEC 27001:2017 gli elementi presenti nella Norma che saranno sottoposti ad Audit saranno 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.*

***INVESTIMENTO ECONOMICO DEL PROGRAMMA***

L’importo delle attività previste è pari a:

Totale Offerta ***Euro 350 + iva***

Prezzo a Voi riservato ***Euro 350 + iva***

***Il costo è comprensivo della redazione di tutti i documenti indicati 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.

L’incarico si rinnova tacitamente ogni anno, salvo diversa comunicazione da inoltrare a mezzo raccomandata entro 90 giorni dalla scadenza, originaria o rinnovata.

**Rapporti operativi:**

GRUPPO CS fornirà un Audit Report, contenenti le informazioni sullo stato di applicazione del Sistema di Gestione della Privacy, oltre alle indicazioni operative, circa le attività da svolgere a carico del Cliente.

**Fatturazione:**

GRUPPO CS emetterà la fattura relativa alle attività sopra indicate, alla sottoscrizione del presente incarico, ovvero al rinnovo annuale dello stesso.

**Condizioni di pagamento:**

***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: xxxx

**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