Consiglio Nazionale
dei Dottori Commercialisti
e degli Esperti Contabili

ALLEGATO 4

PROPOSTA DI COLLABORAZIONE IN MATERIA DI CONSULENZA PRIVACY

-- NOVEMBRE 2022

Carta intestata del professionista

Spett.le

NOME CLIENTE

Via _____ n. __

CAP - Città

Luogo e data

Oggetto: proposta di collaborazione in materia di consulenza privacy.

Spettabile Società,

con la presente di seguito sottopongo la mia proposta di collaborazione in materia di consulenza privacy.

Cordiali saluti

Dott. _____

Carta intestata del professionista

Proposta di collaborazione in materia di consulenza privacy[1]

Il sottoscritto Dott. [inserire], iscritto all'Ordine dei Dottori commercialisti e degli Esperti Contabili di [inserire] al n. [inserire], avente studio professionale in [inserire] alla Via [inserire] n. [inserire], di seguito: "professionista", con la presente comunica il preventivo per l'incarico di collaborazione in materia di consulenza privacy.

Premessa

Le attività che verranno poste in essere dal professionista saranno le seguenti:

- Preliminare attività di risk assessment. Trattasi di "check-up" funzionale all' identificazione dei trattamenti, al censimento delle tipologie di dati personali, di interessati, di finalità, di tempo di conservazione dei dati; mappatura e censimento dei flussi di dati interni ed esterni; all'esame dei documenti e contratti rilevanti ai fini dell'adeguamento normativo; al censimento dei rischi in coordinamento con analisi tecnico-informatica; alla identificazione delle modalità di trattamento (fisiche, organizzative e logiche). Conclude l'attività di assessment la verifica dell'obbligo o dell'opportunità di nomina del DPO.
- *Compliance.* Predisposizione degli adempimenti richiesti nel rispetto della Privacy by Design e Privacy by Default. Il titolare, recependo le indicazioni del Regolamento 2016/679 (di seguito anche: "GDPR"), conseguirà la conformità al medesimo e potrà dimostrare, in caso di attività ispettiva, le misure di sicurezza adottate per la tutela dei dati sottoposti al suo trattamento. La *compliance* comprende la designazione dei ruoli e delle responsabilità con la formalizzazione documentale di incarichi e istruzioni per addetti e responsabili del trattamento *ex* art. 28 GDPR; la predisposizione o revisione dei moduli della privacy e dei documenti contenenti le informazioni *ex* artt. 13 e/o 14 GDPR; la revisione dell' informativa del sito e dei cookie; la predisposizione o revisione della valutazione d'impatto (DPIA) sulla protezione dei dati per i trattamenti *ex* art. 35 GDPR; l'assistenza nelle notifiche dei *data breach*; l'assistenza sulla definizione e attuazione di adeguate misure di sicurezza così come previsto dal GDPR; la realizzazione dei disciplinari interni, la predisposizione del registro dei trattamenti (art. 30 GDPR) e la consegna del modello organizzativo interno; trattamento *ex* art. 28 GDPR; la predisposizione o revisione dei moduli della privacy e dei documenti contenenti le informazioni *ex* artt. 13 e/o 14 GDPR; la revisione dell' informativa del sito e dei cookie; la predisposizione o revisione della valutazione d'impatto (DPIA) sulla protezione dei dati per i trattamenti *ex* art. 35 GDPR; l'assistenza nelle notifiche dei *data breach*; l'assistenza sulla definizione e attuazione di adeguate misure di sicurezza così come previsto dal GDPR; la realizzazione dei disciplinari interni, la predisposizione del registro dei trattamenti (art. 30 GDPR) e la consegna del modello

[1] Nel presente fac-simile ci si è occupati esclusivamente degli aspetti specifici inerenti all'oggetto dell'incarico professionale. Per una più accurata disamina degli elementi essenziali del mandato professionale si rinvia al seguente link: http://www.mandatoprofessionale.it/.

organizzativo interno; la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo (art. 39 GDPR).

- Accountability. Questa attività ha lo scopo di mantenere inalterata nel tempo la conformità del sistema privacy al regolamento. Periodicamente verrà programmata attività di assessment, di audit e di formazione degli addetti e dei responsabili (artt. 29 e 32, co. 4, GDPR) finalizzata alla verifica del recepimento delle istruzioni nonché alla necessità di eventuali modifiche a seguito di cambiamenti indotti dalle mutevoli dinamiche aziendali.

1. Oggetto della proposta

Il Dott. [inserire] si impegna a svolgere per conto di [inserire] (di seguito anche "titolare del trattamento") attività di consulenza in materia di privacy.

L'attività consiste nella progettazione e realizzazione di un modello organizzativo e del suo mantenimento, attraverso lo svolgimento delle seguenti fasi:

- *data protection gap analysis*: mappatura degli ambiti e definizione dei processi di ciascun ambito che include:
    - esame e censimento tipologie di dati personali, di interessati, di finalità, di tempo di conservazione dei dati;
    - censimento flussi di dati interni ed esterni;
    - esame dei documenti e contratti rilevanti ai fini dell'adeguamento normativo al GDPR;
    - censimento rischi (in coordinamento con analisi tecnico-informatica);
    - censimento rischi sito e pagine social;
    - supervisione nella redazione delle DPIA;
- monitoraggio designazioni e relativa formazione: titolare, responsabile di trattamento e addetti, amministratore di sistema, qualora presente;
- informative: revisione informativa sito (include cookie); dipendenti, collaboratori e ruoli aziendali (include diciture footer e-mail); revisione informativa fornitori, clienti ed ogni ambito relativo al trattamento della articolazione organizzativa del titolare;
- consenso: mappatura dei trattamenti per cui è necessaria la base giuridica del consenso e definizione di un sistema di acquisizione, controllo e conservazione degli stessi;
- notifiche e comunicazioni: assistenza nella notifica; assistenza nella notifica *data breach*; assistenza nella comunicazione *data breach* agli interessati, assistenza nella richiesta di esercizio dei diritti da parte degli interessati;
- sicurezza: assistenza sull'attuazione delle misure minime di sicurezza in caso di enti pubblici e delle misure adeguate in caso di titolari privati; assistenza sull'attuazione delle misure previste dal GDPR in materia di amministratori di sistema;
- policy e disciplinari interni: predisposizione *privacy policies* adempimenti di dipendenti e

collaboratori - policy sicurezza informatica (con l'assistenza esterna di un vostro consulente); disciplinare interno per utilizzo di posta elettronica e Internet (social inclusi); disciplinare interno su procedure da svolgere nel caso di data breach; disciplinare interno su procedure da svolgere nel caso di esercizio dei diritti dell'interessato;

- *accountability*: assistenza predisposizione registro trattamenti.

2. Obblighi del professionista

Il professionista si impegna a svolgere le attività di cui al punto 1 con la massima diligenza, secondo le modalità e le condizioni ivi previste.

Le attività di cui al punto 1 vengono eseguite dal professionista esclusivamente su dati e documenti predisposti e consegnati dal titolare del trattamento.

3. Attività di audit

Il Dott. [inserire] si impegna a supervisionare il modello organizzativo privacy del titolare del trattamento. Questa attività consiste nella realizzazione di verifiche ispettive interne, nella progettazione e manutenzione del sistema privacy, in conformità alle disposizioni vigenti ed attenendosi alla normale diligenza richiesta dalla prassi.

Qualora la documentazione consegnata dal titolare del trattamento dovesse risultare incompleta, incomprensibile o carente, il Dott. [inserire] potrà anche astenersi dall'esecuzione dell'incarico, previo preavviso da inviare presso la sede del titolare del trattamento, anche a mezzo di posta elettronica certificata.

Il Dott. [inserire] si riserva di utilizzare sistemi di elaborazione elettronica dei dati (software) ed apparecchi per l'elaborazione elettronica degli stessi (hardware), idonei alle necessità del titolare del trattamento.

Previa comunicazione al titolare del trattamento, nell'esecuzione dell'incarico il Dott. [inserire] si potrà avvalere, sotto la propria responsabilità, di sostituti, ausiliari, collaboratori e personale dipendente dei quali fornirà, su richiesta, il *curriculum vitae*.

4. Esclusioni

L'attività di consulenza non prevede: gli interventi tecnici che occorre realizzare per proteggere il sistema di gestione dei dati (a titolo esemplificativo ma non esaustivo: attività di manutenzione e adeguamento della rete, la fornitura dei supporti HW e SW ove si rendessero necessari).

È esclusa dalla presente proposta l'assistenza legale esterna al DPO e al titolare del trattamento nel caso di ispezioni e verifiche sulla conformità alla normativa in ambito privacy. Tale attività verrà quantificata, preventivata e fornita separatamente su specifica richiesta.

5. Obblighi del titolare del trattamento

Il titolare del trattamento si impegna a fornire tutte le informazioni e i dati necessari:

- all'espletamento del presente incarico, assumendosi la responsabilità per le informazioni eventualmente omesse o errate che non dovessero consentire un corretto adempimento dell'obbligazione contrattuale;
- per effettuare la corretta valutazione dei rischi, nonché quelle relative a variazioni e/o modificazioni di carattere tecnico-organizzativo rilevanti ai fini normativa privacy.

Il titolare del trattamento si impegna a comunicare tempestivamente al professionista, a titolo esemplificativo e non esaustivo, le seguenti eventuali circostanze:

- variazione dei responsabili del trattamento e/o variazioni dei soggetti autorizzati e/o incaricati;
- variazioni degli asset (archivi, sedi, server, pc, smartphone e tablet);
- variazioni dell'organizzazione, tecniche e di tutto quanto possa assumere rilevanza al fine delle attività oggetto di contratto.

Tali eventuali variazioni dovranno essere comunicate rigorosamente per iscritto entro e non oltre cinque (5) giorni dalla loro attuazione al fine di consentire di provvedere tempestivamente alla rielaborazione di quanto necessario ai fini dell'adeguamento.

6. Durata dell'incarico

Il presente contratto ha durata di 3 anni ed è rinnovabile tacitamente salvo disdetta da comunicare entro 30 gg. dalla scadenza.

7. Responsabilità

È esclusa ogni responsabilità del Dott. [inserire]:

- qualora il titolare del trattamento dovesse assumere un comportamento difforme da quanto suggerito e consigliato al fine di ottemperare agli obblighi della normativa vigente in materia di privacy;
- relativa al mancato adeguamento dei sistemi informatici (ICT) e delle misure di sicurezza organizzative, tecniche, informatiche, logistiche e procedurali da parte del titolare del trattamento;
- qualora il titolare del trattamento dovesse rendersi inadempiente a uno o più obblighi di cui al punto 5.

8. Corrispettivo

Il corrispettivo per questo incarico è stabilito in base a quanto previsto dettagliatamente nell'Allegato "A" Stima del piano di lavoro, che forma parte integrante del presente preventivo.

Il corrispettivo sarà corrisposto alle seguenti scadenze:

Gap analysis e adeguamento:

- il 30 % alla accettazione della presente proposta;
- il restante 70% del corrispettivo con l'avanzamento dei lavori definito con i referenti del titolare del trattamento.

Mantenimento

Il corrispettivo del mantenimento sarà corrisposto entro le date previste del verbale di riesame e delle attività di audit e formazione periodica.

9. Variazioni del corrispettivo

Il Dott. [inserire] nel corso del rapporto, avrà facoltà di variare l'importo del corrispettivo nel caso in cui le prestazioni a favore del titolare del trattamento divenissero più impegnative e/o più complesse e/o più onerose. In tal caso dovrà dare un preavviso scritto di variazione di almeno trenta (30) giorni ed il disaccordo del cliente costituirà motivo di giusta causa per recedere dal contratto. Il titolare del trattamento, nel corso del rapporto, avrà facoltà di richiedere la riduzione dell'importo del corrispettivo, nel caso in cui la sua attività abbia subìto una riduzione rispetto a quella del precedente anno: in tal caso il titolare del trattamento dovrà farne richiesta scritta al professionista, il quale si riserva il termine di trenta (30) giorni per l'approvazione. Il mancato accordo costituirà motivo di giusta causa per recedere dal contratto.

10. Recesso e risoluzione per inadempimento

È fatta salva la facoltà per ciascuna delle parti di recedere in qualunque momento dal presente contratto, con l'obbligo di darne preavviso all'altra parte con lettera raccomandata A.R. spedita centottanta (180) giorni prima della data dell'effettivo recesso.

Il Dott. [inserire] ha diritto di recedere in qualunque momento dal presente contratto, previo preavviso scritto di trenta (30) giorni, tramite raccomandata A.R., per i seguenti motivi, che costituiranno senz'altro giusta causa, qualora il titolare del trattamento:

- risulti inadempiente rispetto agli obblighi di cui al punto 5;
- abbia fornito al professionista documenti e reso dichiarazioni incomplete, incomprensibili, false e/o alterate;
- non consegni in tempo i dati e le comunicazioni necessarie;
- risulti inadempiente circa gli obblighi assunti rispetto al pagamento del corrispettivo pattuito.

Il titolare del trattamento ha diritto di recedere dal presente contratto previo preavviso scritto di trenta (30) giorni, tramite raccomandata A.R., in caso di cessazione dell'attività.

In caso di inadempimento da parte di uno dei contraenti alle obbligazioni previste dal presente incarico, l'altro contraente potrà intimare per iscritto, mediante comunicazione specifica e

circostanziata, all'inadempiente di porvi rimedio entro il termine ordinatorio di 30 gg. Decorso inutilmente tale termine, la parte intimante potrà dichiarare per iscritto la risoluzione del contratto o della sola parte cui è relativo l'inadempimento, con riferimento agli obblighi su disciplinati.

Il diritto di avvalersi della risoluzione di diritto a norma dell'art. 1456 c.c., in simili circostanze, resta esercitabile in qualunque momento se la parte inadempiente non ponga rimedio all'inadempimento.

In caso di risoluzione anticipata verranno corrisposti dal titolare del trattamento solo gli emolumenti per le prestazioni relative al periodo intercorrente tra la data della raccomandata e dell'effettivo recesso.

11. Varie

Nessuna modifica, aggiunta o deroga alle disposizioni del presente atto può avere efficacia se non risulti per iscritto con la sottoscrizione di entrambe le parti.

12. Rinvio

Per tutto quanto non esplicitamente previsto dal presente atto, si fa riferimento alle leggi, usi e consuetudini vigenti in materia.

13. Accordo di Riservatezza per tutte le informazioni fornite dal Titolare del trattamento e per il trattamento dei dati

Il Dott. [inserire] e il titolare del trattamento dichiarano con la presente di essere consapevoli che, a seguito dell'incarico conferito con il presente atto, potranno venire a conoscenza di dati, informazioni e notizie in genere, aventi natura riservata e si impegnano a mantenere il più stretto riserbo su quanto ricevuto, nonché su qualsiasi altra notizia, confidenza e/o informazione, nel più ampio significato del termine, appresa.

I dati raccolti saranno trattati, ai sensi del Regolamento 2016/679/UE e del d.lgs. n. 196/2003 e ss.mm.ii., esclusivamente nell'ambito dell'espletamento del presente incarico, in modo da garantirne la sicurezza, riservatezza e liceità.

Data Firma per accettazione

Carta intestata del professionista

Allegato "A" Stima del piano di lavoro

1	**impostazione progetto n. ore**	**53**
	Interviste n. ore	15
	definizioni ambiti n. ore	14
	definizione processi e trattamenti per ciascun ambito individuato n. ore	24
	Provisioning e profilatura utenti per ciascun ambito individuato n. ore	**23**
	Individuazione e designazioni soggetti coinvolti n. ore	15
	definizione asset (infrastruttura e applicativi) n. ore	8
3	**DPIA per ciascun ambito individuato n. ore**	**24**
	Valutazione di impatto n. ore	22
	Definizione rischi lordi n. ore	2
4	**Misure di sicurezza per ciascun ambito individuato n. ore**	**47**
	Definizione Livello rischi residui art 32 e 35 n. ore	15
	Procedure n. ore	15
	Istruzioni n. ore	15
	Piani di emergenza n. ore	2
5	**Document Compliance per ciascun ambito individuato n. ore**	**39**
	Assistenza predisposizione registri obbligatori n. ore	24
	mappatura e aggiornamento della modulistica e documentazione interna n. ore	15
6	**Formazione per ciascun ambito individuato n. ore**	**32**
	One to One per figure apicali n. ore	8
	Altre modalità per la restante articolazione aziendale compresa la formazione a distanza n. ore	24
7	**Pareri scritti n. ore**	**15**
8	**Sopralluoghi e incontri presso Vs. Azienda n. ore**	implicito
9	**Piattaforma Cloud per la gestione degli adempimenti, della formazione e delle nomine (ad esclusione del costo della firma elettronica automatica) n. ore**	Implicito
	Totale sviluppo in ore	**233**
	Occurency in percentuale espressa in ore (10%)	23
	Gestione progetto in percentuale espressa in ore (5%)	12
	Totale generale in ore	**268**
	Tariffa oraria a voi riservata	50
	Proposta economica (IVA ESCLUSA)	**13.397,50**
	Condizioni a voi riservate (Iva esclusa)	**10.800,00**