Doc.1
Allegato al contratto

Franco, Pirro & Partners, Società tra Professionisti s.r.l.
Consulenza Legale e Commerciale, Esperti in privacy e protezione dati
Riconosciuto tra gli "Studi dell'anno 2021" nella ricerca Sole 24Ore - Statista
Via de Cesare, 37 - 74123 - Taranto (TA)
Sede di Bari: via Cancello Rotto, 3/B, cap 70125
P.Iva 03176190738 - C.F. 03176190738

FRANCO, PIRRO & PARTNERS

PREVENTIVO nr. 16/2022 del 14/04/2022

P.IVA 07086860728
CF 07086860728

DESTINATARIO
SixT SpA
P.zza XX Settembre 32
70033 Corato (BA)

OGGETTO
Esternalizzazione funzione DPO

CODICE	DESCRIZIONE	QUANTITÀ	IMPORTO
DPO01	Esternalizzazione funzione del Responsabile Protezione Dati ex art.37 GDPR Esternalizzazione delle attività di adeguamento al nuovo Regolamento Generale sulla Protezione Dati Reg. 2016/679/UE	1 anno	€ 1.000,00

Franco, Pirro & Partners STP S.r.l.

NOTE

Rimborso a piè di lista per le trasferte fuori Taranto.
Il preventivo è valido sino al 10 maggio 2022.
I compensi indicati si intendono al netto degli oneri accessori di legge (RSG, CAP ed IVA).
Pagamento all'atto del conferimento dell'incarico

Firma per accettazione
S.I.x T. S.p.A. - A. D. Giuseppe Pirro

MODALITÀ DI PAGAMENTO
Bonifico Bancario
IBAN: IT64X0542415800000001002146
Intestato a: Franco, Pirro & Partners S.T.P. S.r.l.

Franco, Pirro & Partners, Società tra Professionisti s.r.l.
www.francopirro.it - amministrazione@francopirro.it
tel: +39 0805899034

Premessa

Il Regolamento UE 2016/679, il GDPR (General Data Protection Regulation) tutela il diritto alla privacy delle persone fisiche, bilanciandolo con il diritto dell'impresa a trattare i dati raccolti, se compie i passi corretti e conformi alla legge.

Il Regolamento riguarda le Aziende, gli Studi professionali, le Ditte individuali, gli Enti pubblici e quelli privati che trattano i dati dei cittadini UE ed è efficace dal 25.05.2018.

Invece, il "vecchio" d.lgs. 196/2003, meglio conosciuto come "Codice Privacy", è stato emendato con il d.lgs. 101/2018 per renderlo conforme al GDPR: parte delle sue disposizioni sono state abrogate poiché in palese conflitto con la normativa europea, mentre un'altra parte è stata armonizzata con le vigenti disposizioni in materia. La protezione dei dati penali, infine, è ora regolata dal d.lgs. 51/2018 (attuativo della direttiva europea n. 680/16 che, a sua volta, abroga la decisione quadro 2008/977/GAI del Consiglio Europeo): dunque, questo tipo di informazioni dovrà essere trattato con maggiori cautele anche da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati.

Dunque, chi ancora non si è adeguato alle nuove disposizioni normative deve urgentemente attivarsi per analizzare tutta la propria organizzazione e implementare processi e sistemi di sicurezza per renderla conforme.

Le Opportunità del GDPR e le ragioni fondanti

Gli abitanti connessi nel 1995, quando venne emanata per la prima volta la normativa sulla privacy (Dir. 95/46/CE), erano l'1%. Oggi in Italia gli utenti connessi sono 30.21 milioni su 59.8 milioni di abitanti, pari al 51%. In Europa il 67,3% è connesso a Internet.

La mole di dati trattati in generale è elevatissima e, ovviamente, su internet è enorme. Le potenzialità della profilazione di questi dati sono incredibili. Il modello di business adottato da ogni azienda nel momento stesso in cui incrocia informazioni personali compete con la protezione di un diritto fondamentale della persona.

Con il nuovo regolamento europeo le grandi potenzialità dello sfruttamento dei dati possono essere perseguite dalle aziende a patto che i dati vengano gestiti con modalità e sistemi conformi alle norme.

IL GDPR, PERTANTO, PUÒ ESSERE UNA GRANDE OPPORTUNITÀ

Cosa cambia per le Aziende

Il GDPR impone ad Aziende ed Enti pubblici una grande autodeterminazione, una forte responsabilizzazione e la libertà nelle scelte strategiche ed operative nella gestione dei dati. È una delle maggiori novità rispetto al precedente Codice Privacy.

Ad esempio, non è più necessario notificare al Garante trattamenti di carattere delicato, ma deve essere tenuta traccia del ciclo di vita dei dati in modo da averne completo controllo e dimostrabilità della gestione.

Coloro che vedono o hanno visto il trattamento dei dati e la gestione della sicurezza non come un adempimento meccanico e formale, ma come un'occasione di crescita e di miglioramento della propria posizione sul mercato, possono cogliere o, ancora, hanno già colto una opportunità importante.

Cosa succede in caso di violazione (Data Breach)

Un **Data Breach** è una violazione dei propri sistemi informatici o dei propri archivi cartacei che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Un Data Breach, quindi, può essere una violazione riguardante asset di varia natura e contenenti dati la cui perdita può determinare lesioni dei diritti o delle libertà delle persone a cui quei dati si riferiscono. Oggi, in piena vigenza del GDPR, il Titolare del trattamento che ha subito una violazione o una perdita dei dati personali deve comunicare entro 3 giorni (72 ore) l'accaduto all'Autorità Garante e anche a tutti gli interessati coinvolti.

L'azienda deve, quindi, dotarsi di strumenti appropriati sia di *governance*, sis di controllo e verifica che consentano la tempestiva scoperta delle violazioni e la relativa corretta gestione.

Non basta rispettare le norme in materia di protezione dei dati personali, ma, in ossequio del principio di *accountability*, i Titolari dovranno dimostrare di essere consapevoli delle modalità di trattamento e di conservazione degli stessi e di aver fatto tutto il possibile per scongiurare l'evento dannoso.

Oltre alle eventuali sanzioni (v. oltre) il verificarsi di una violazione può causare le seguenti conseguenze:

- un danno reputazionale e di immagine che può portare a gravi conseguenze sull'attività dell'azienda;

- azioni di responsabilità per il mancato rispetto delle pattuizioni contrattuali con altri titolari o contitolari;

- azioni risarcitorie da parte degli interessati (clienti, dipendenti, fornitori) i cui dati sono stati oggetto del Data Breach.

Le sanzioni

Il regime sanzionatorio è molto pesante. Le sanzioni arrivano fino a 20 milioni di euro o al 4% del fatturato globale se il primo limite dovesse risultare inadeguato.

Chiunque subisca un danno materiale o immateriale causato da una violazione ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento. Qualora più Titolari o responsabili siano coinvolti nello stesso trattamento e siano, quindi, responsabili dell'eventuale danno causato dal trattamento, tutti risponderanno in solido con gli altri per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato.

L'Autorità di controllo, oltre a comminare sanzioni di tipo pecuniario, può anche imporre al Titolare l'implementazione di misure procedurali o tecniche di natura correttiva, limitando, sospendendo o addirittura bloccando i trattamenti in corso sino all'adempimento delle prescrizioni.

Con il D.Lgs. 101/2018, inoltre, è stato inasprito il sistema sanzionatorio penale. Accanto alle confermate fattispecie già previste dal Codice Privacy sono stati introdotti nuovi reati, ampliandone così la lista a:

- *trattamento illecito dei dati;*
- *comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala;*
- *acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala;*
- *falsità nelle dichiarazioni all'Autorità Garante;*
- *interruzione dell'esecuzione dei compiti e poteri dell'Autorità Garante;*
- *inosservanza dei provvedimenti dell'Autorità Garante.*

Le funzioni coinvolte – Il DPO

Accanto alle figure del Titolare del trattamento (*controller*) e del Responsabile del trattamento (*processor*) il GDPR introduce la nuova figura del ***Data Protection Officer (DPO)*** o, in italiano, Responsabile della Protezione dei Dati (RPD), che è il vero perno e punto chiave della gestione della privacy e della sicurezza dei dati. Si tratta, infatti, di una figura particolarmente competente e dotata di conoscenze multidisciplinari che vanno dalla preparazione giuridica (conoscenza delle norme) a quella tecnico/operativa, di modo che possa relazionarsi con tutte le funzioni aziendali per comprendere analizzare i rischi correlati ad ogni trattamento.

Il DPO può essere una figura interna all'azienda appositamente reclutata e contrattualizzata, ma anche un ente esterno provvisto delle necessarie competenze, come Franco, Pirro & Partners.

Perché farlo

Il governo del rischio e la gestione della privacy e della sicurezza dei dati, considerando tutte le componenti aziendali come un *unicum* alimentato da ognuna di esse, consentono all'Azienda di produrre un risultato complessivo rappresentato dai fatturati, dagli utili, dalla riconoscibilità di marca, dall'affezione dei clienti, dal rispetto dei concorrenti, dalla stima dei fornitori, dalla considerazione generale degli stakeholder, dalla fiducia degli azionisti. L'Azienda, dunque, può:

- ✓ **Conservare la migliore immagine (*brand awareness*)**: i clienti, i fornitori, i subfornitori, i partner, gli outsourcer, saranno felici di lavorare con quell'azienda;

- ✓ **Proteggere i dati di modo da proteggere il business**: la realizzazione di processi dinamici, progettati e adeguati in modo continuativo e conforme alla protezione dei dati consente anche la protezione del know-how aziendale;
- ✓ **Attirare le migliori risorse**: lavorare per l'azienda conforme, ma soprattutto ben attrezzata con un sistema efficace di gestione della privacy, è ambito e desiderato: si può, quindi, assicurarsi le migliori risorse del mercato;
- ✓ **Rassicurare i dipendenti**: processi efficaci, funzionali e rispettosi dei dati creano un ambiente di lavoro positivo che aumenta affezione e fedeltà dei dipendenti, e, perché no, anche la loro produttività;
- ✓ **Evitare costosi contenziosi**: le violazioni dei dati personali attirano cause civili lunghe e costose da parte di enti di protezione dei consumatori;
- ✓ **Evitare le sanzioni**: l'art. 83 prevede sanzioni elevatissime: fino a 20 mln di euro o fino al 4% del fatturato annuo se superiore.

I servizi di Franco, Pirro & Partners

Franco, Pirro & Partners basa i propri servizi su logiche di prevenzione, riduzione e trasferimento del rischio e su processi di Risk Governance, adottando le moderne metodologie di Risk Management e gli strumenti più pertinenti al caso del cliente (p. es. tool di analisi comportamentale, *big data analytics*, intelligenza artificiale, mappe del rischio) per realizzare il più adeguato action plan, tarato sulle esigenze e sulle dimensioni dell'azienda al fine di raggiungere e garantire dinamicamente la conformità agli standard richiesti dalle norme sulla privacy e sulla sicurezza del trattamento.

I nostri clienti possono contare su:

Esternalizzazione dei servizi privacy: outsourcing per l'assistenza alle funzioni interne per il rispetto delle normative in tema di privacy e protezione dati;

Data Protection Officer: outsourcing di Data Protection Officer e la consulenza e assistenza ai Data Protection Officer interni in base a un contratto di servizi;

Sicurezza informatica: piani di realizzazione e assessment di sicurezza informatica;

Formazione: per personale coinvolto nei processi di trattamento privacy e sicurezza dei dati, anche on site e on line;

Web site & e-Commerce: analisi e messa a norma dei siti web in ambito privacy e protezione dati, cookies, consulenza e assistenza ai fini rispetto delle disposizioni vigenti in materia di tutela dei consumatori e del copyright, verifica del rispetto normative speciali per singolo industry (es. sanità, investigazioni, ecc.);

App & Software: analisi e messa a norma delle *"mobile application"* e dei software in ambito privacy e protezione dati, consulenza e assistenza ai fini rispetto delle disposizioni vigenti in materia di tutela dei consumatori e del copyright, normative speciali per singolo *industry*.

Chi siamo

Franco, Pirro & Partners è un team multidisciplinare composto da avvocati esperti in diritto privacy e internet, commercialisti esperti in gestione e pianificazione organizzativa aziendale, ingegneri e tecnici informatici, sociologi, auditor esperti di standard ISO, specialisti ICT, specialisti HR, molti dei quali specializzati presso l'Università di Bologna con cui collaborano attivamente. La presenza nelle più importanti città italiane ci consente il contatto diretto sul territorio nazionale.

Come operiamo

Franco, Pirro & Partners lavora fianco a fianco con il personale interno e i consulenti esterni dell'Organizzazione cliente, individuando le migliori soluzioni realizzate su misura per le esigenze contingenti di adeguamento e per la realizzazione di un sistema di gestione dinamico che consenta l'ottenimento e il mantenimento costante della conformità.

La Società

La Società tra Professionisti Franco, Pirro & Partners STP S.r.l. è stata creata dall'Avv. Elio Franco e dal Dott. Luigi Pirro con il preciso intento di fornire consulenza di alta qualità e professionalità ai propri clienti in materia di Privacy e Protezione dati, Compliance normativa in particolare per gli operatori del web (web site, e-commerce, blog, ecc.) e consulenza strategica per le aziende. Cura anche la tutela del diritto d'autore e della proprietà industriale, le problematiche connesse agli scambi commerciali internazionali, al diritto del lavoro e la difesa in giudizio dei propri clienti

Annovera tra i suoi clienti Enti Pubblici o Concessionari di servizi pubblici (istruzione, trasporto, energia), importanti aziende operanti in Italia (automotive, sanità convenzionata e non, ristorazione, spedizioni marittime ed internazionali, consulenza professionale, alberghiere, turistiche, farmacie, ecc), Associazioni ed enti del III settore (onlus, sportive, di volontariato), Professionisti (commercialisti, avvocati, psicologi, ingegneri, progettazione, amministratori).

I fondatori

Elio Franco

Avvocato, esperto di diritto delle nuove tecnologie, privacy e diritto d'autore online. Segue con interesse lo sviluppo delle tecnologie, soprattutto dal punto di vista della sicurezza.

Specializzatosi all'Università di Bologna con il Corso di Alta Formazione in Websecurity e Privacy Officer, segue diversi enti privati come consulente privacy e DPO.

Ha all'attivo alcune pubblicazioni scientifiche in materia ed è relatore in convegni e seminari che riguardano le problematiche legali sul web. Scrive per SaggiaMente.com. È cofondatore di anormadilegge.it e di databased.it.

Luigi Pirro

Dottore Commercialista dal 1989, ha conseguito un master in Business Administration, ed uno in Information Technology; esperto in banking litigation e in progettazione per l'accesso ai fondi diretti europei, revisore legale, gestore crisi da sovraindebitamento per l'Organismo dei Commercialisti di Bari.

Specializzato all'Università di Bologna con il Corso di Alta Formazione in Websecurity e Privacy Officer, assiste clienti privati come consulente privacy e Responsabile Protezione Dati (DPO).

Docente in corsi di formazione e relatore in convegni, ha maturato esperienze di management in molteplici industry come automotive, food, ICT, editoria professionale. Scrive sul web articoli su Privacy, Finanza UE e pratica bancaria. È cofondatore di a norma dil egge.it e di databased.it

Le azioni di Franco, Pirro & Partners per SIxT

Sulla base delle informazioni in nostro possesso, abbiamo sintetizzato gli interventi che riteniamo necessari, riservandoci di specificare ulteriormente le attività da realizzare nel corso dell'esecuzione della prestazione.

Le attività elencate di seguito si inseriscono in un ampio progetto che prevede fasi di rilevazione e analisi, fasi di intervento e modifica per raggiungere la conformità, fasi di progettazione per adeguare e rendere conformi i nuovi servizi, fasi di monitoraggio e controllo.

Fasi del progetto	
Fase A Analisi	Analisi del contesto aziendale e di lavoro sui flussi di dati già rilevati. Controllo dell'organigramma privacy
Fase B Controllo	Controllo documentazione già da predisposta: • Informative sul trattamento dati per gruppo di interessati (clienti, dipendenti, fornitori); • Dichiarazioni di raccolta del consenso; • Atti di designazione dei soggetti autorizzati (per dipendente); • Atti di designazione dei responsabili esterni del trattamento; • Procedure per i trasferimenti di dati all'estero.
Fase C Verifica delle procedure	Controllo dell'implementazione del modello di gestione privacy
	Controllo del modello per l'esercizio dei diritti degli interessati
	Controllo del modello di gestione dei Data breach
	Controllo del regolamento informatico

Attività opzionali a richiesta	
❑ **Formazione (€ 250,00 a modulo di due ore)**	Formazione del personale su norme e procedure in materia di privacy e protezione dati. Con test finale e rilascio attestato di partecipazione. In aula o webinar in modalità sincrona.
❑ **Analisi dei rischi (€ 200,00 /ora uomo)**	Risk assessment con redazione piano dei rischi e report criticità
❑ **Assistenza nella progettazione di nuovi servizi (€ 200,00 /ora uomo)**	Privacy by design: conformità fin dalla progettazione di nuovi servizi e prodotti
	Privacy by default: conformità per impostazione predefinita
❑ **Audit periodico (€ 500,00 /audit)**	Attività di verifica dell'adeguamento oltre quella inclusa nel preventivo allegato

Condizioni e modalità

- Durata: 1 anno;
- Compensi professionali: vedi preventivo allegato;
- Modalità contrattuale: contratto di conferimento incarico professionale;
- Modalità di pagamento: con Bonifico SEPA;
- I compensi sono indicati al netto di IVA, C.A.P., R.S.G.[1];
- Valuta: Saldo al conferimento dell'incarico.

Luogo e Data

Accettazione del piano di lavoro e del preventivo allegato
(attività prescelte con X)

Franco, Pirro & Partners STP S.r.l.

(timbro e firma)

SIXT spa

[1] *RSG - Rimborso spese generali: come per legge pari al 15% dell'onorario (Art. 2 D.M. 55/2014)*
CAP – Cassa di previdenza professionale: come per legge pari al 4% dell'onorari