ESTRATTO PUBBLICO D.U.R.P.
Documento Unico Rispondenza Privacy

AUTOCERTIFICAZIONE RISPONDENZA NORMATIVA GDPR

Gentile cliente,
teniamo particolarmente alla riservatezza, integrità e disponibilità dei dati personali che trattiamo susseguentemente le attività consulenziali che ci affidate. Per questo motivo vorremmo condividere – attraverso questo documento - le informazioni principali sulle modalità di trattamento e sulle misure adottate per tutelare i vostri dati personali ed aziendali.

A fronte dei rapporti che intercorrono tra le nostre realtà lavorative ed a fronte dell'entrata in vigore del Regolamento Generale per la Protezione dei Dati 2016/679, normativa che a livello europeo regola il trattamento dei dati (di qui in avanti la "normativa" o il "GDPR"), La informiamo che:

1. il nostro Ente ha preso coscienza della normativa in tutte le sue parti con particolare riferimento ai principi normativi ivi compreso il principio di "accountability" (responsabilizzazione), in tal modo raggiungendo la "consapevolezza" delle prescrizioni normative e del loro impatto sui trattamenti che effettuiamo sui vostri dati;
2. il nostro personale dirigente e consulenziale – o comunque rientrante in maniera determinante nel processo produttivo – è oggetto di formazione specifica per l'esecuzione delle attività professionali affidateci;
3. il nostro Ente si è adoperato per analizzare lo stato corrente di tutti gli elementi che intercorrono nei trattamenti dati da noi effettuati;
4. gli elementi che non rispettavano la normativa sono costantemente corretti, eliminati o sostituiti in modo e maniera da risultare ora a norma.

In particolare vorremmo segnalarLe che:

1. i dati personali che trattiamo sono relativi all'anagrafica delle vostre risorse umane – in massima parte dati pubblici – comprensivi di nome, cognome, email aziendale, numero di telefono aziendale (talvolta, stante le necessità operative e relativamente a talune risorse umane, potremmo assumere anche il numero di cellulare);
2. i dati relativi alla vostra azienda acquisiti durante le sessioni di audit, ancorché non rientranti nella definizione di dato personale, sono trattati con le stesse cautele richieste dal GDPR per i dati personali;
3. le risorse umane che operano le sessioni di trattamento sono costantemente rese edotte circa gli obblighi che incombono sui trattamenti effettuati ed hanno sottoscritto debito accordo di riservatezza circa i dati che ci affidate in qualità di Responsabile Esterno;
4. le risorse umane del nostro Ente sono costantemente informate e formate al fine di oggettivamente limitare eventuali rischi sui dati a noi affidati;
5. le nostre strutture informatiche (ubicate su server proprietari che ospitano servizi della nostra società) sono state messe a norma e l'accesso alle stesse è regolamentato da un sistema di sicurezza previo l'inserimento delle corrette credenziali elettroniche;
   sono stati adottati livelli di sicurezza in modo che un consulente possa visionare unicamente le pratiche che ha in gestione mentre solo l'amministratore e la segreteria possono visionare, redistribuire, accedere a tutte le pratiche trattate dalla nostra società;
6. le nostre strutture informatiche sono costantemente aggiornate, manutenute, sostituite (con particolare riferimento ai server che sono periodicamente sostituiti), compatibilmente con le dinamiche dell'Ente ed i diritti e le libertà degli interessati, al fine di oggettivamente ridurre i rischi che incombono sui dati a noi affidati con riferimento a rischi relativi a:
   - accessi abusivi (l'accesso amministrativo al server è dotato di doppia autenticazione);
   - distruzione, perdita, modifica non autorizzata (esistono copie in cartelle crittografate dei dati necessari per ridurre la perdita di dati in caso di danno fortuito o doloso);
   - divulgazione non autorizzata (l'accesso alla pratica da parte del consulente è dotato di due livelli di sicurezza, i server sono ubicati in una delle più importanti server farm italiane nei

confronti della quale nutriamo fiducia circa la gestione corretta delle "best practice" di sicurezza);
    - accesso non consentito, sia esso accidentale che illegale;
7. le nostre strutture informatiche sono oggetto di valutazione al fine di assicurare la riservatezza, l'integrità e la disponibilità dei dati nonché la resilienza dei sistemi;
8. l'efficacia delle misure di sicurezza è regolarmente verificata attraverso opportune procedure, studi, verifiche tecniche, implementazioni;
9. sono state create apposite procedure per identificare i data breaches (accessi abusivi ai dati) e, conseguentemente, informarvi senza ingiustificato ritardo circa quali dati, se del caso, sono stati oggetto di accesso abusivo; nello specifico ogni pratica oggetto di accesso segnala al consulente l'avvenuto accesso e tutti i movimenti del soggetto che ha avuto accesso alla pratica sono registrati;
10. i locali ove vengono effettuati i trattamenti sono stati dotati di modalità e/o di misure tendenti a limitare l'accesso da parte di personale non autorizzato: tutte le nostre riunioni si tengono unicamente nella sala riunioni;
11. i dati a noi affidati sono custoditi in conformità con quanto prescritto dalla normativa e sono oggetto di periodico backup multiplo;
12. i supporti che ospitano i backup sono oggetto di accesso limitato; i notebook contenenti i vostri dati sono crittografati con la tecnologia bitlocker ovvero anche in caso di perdita i dati in essi contenuti non saranno ricostruibili;
13. l'eventuale trasferimento dei dati all'estero o verso organizzazione internazionale è stato identificato ed armonizzato con le prescrizioni del GDPR; ci siamo premurati di detenere i dati in strutture tecnologiche italiane (i nostri server); le caselle email sono su server di posta di fornitore di servizi italiano operante su server di proprietà ubicati in Italia; non abbiamo fornitori o sub-responsabili (vedi tabella a seguire) che operano fuori Italia;
14. viene effettuata – durante gli audit – una verifica dei dati trattati per verificarne l'esattezza nonché è stata verificata l'effettiva necessita di trattamento di tutti i dati acquisiti e, se del caso, i dati non rispettanti il principio di minimizzazione sono cancellati dai nostri elaboratori;
15. è stata effettuata una verifica della finestra temporale di trattamento dei dati e, se del caso, i dati eccedenti questo periodo di conservazione sono stati cancellati dai nostri elaboratori; i supporti cartacei contenenti detti dati sono periodicamente digitalizzati, inseriti nella directory dedicata alla vostra azienda, quindi distrutti seguendo le modalità di cui sopra;
16. i dati saranno cancellati anche susseguentemente la risoluzione del contratto di consulenza che ci avete affidato, fatti salvi i casi rientranti nella base giuridica di legittimo interesse e/o in ottemperanza di norme comunitarie o nazionali.

Elenco dei responsabili di cui ci avvaliamo.	
Amministratore di Sistema	Interno
Consulente al trattamento	Interno ed Esterno
Consulenti IT per analisi struttura IT cliente	Esterno (usato previo assenso preventivo cliente)

Laddove utilizzassimo sub-responsabili diversi da quanto sopra riportato, sarà nostra cura informarvi: nel caso in cui desideriate essere preventivamente informati, vi chiediamo di notificarci la vostra richiesta inviandoci una email all'indirizzo segreteria@projectconsult.it

Certi di rendere un servizio gradito, oltre che obbligatorio per legge, Vi inviamo la presente al fine di dichiarare che il nostro Ente.
RISULTA SODDISFARE QUANTO RICHIESTO DAL REGOLAMENTO EUROPEO PER IL TRATTAMENTO DEI DATI PERSONALI 2016/679.
A fronte di quanto sopra, siamo in grado di ricevere e trattare i dati che ci vorrete affidare.

Sistema qualità privacy *sviluppato con il supporto di*:
PROJECT CONSULT
www.projectconsult.it
info@projectconsult.it

è un servizio in collaborazione con **www.leggesullaprivacy.it**