

# **ANALISI E VALUTAZIONE DEI RISCHI E SOLUZIONI OPERATIVE IN MATERIA DI PRIVACY**

(Regolamento UE n. 2016/679, del 27/4/2016)

Titolare del trattamento: RAG. PAOLO MORETTI  
S.E.C.AL. S.p.A. (SOCIETA' ENTRATE COMUNE DI ALGHERO)

Via Sant'Anna 07041 Alghero

Codice fiscale titolare: MRT PLA 61L21 A192A

## **PREMESSA**

La presente analisi e valutazione viene effettuata al fine di verificare il rispetto delle disposizioni contenute nel Regolamento UE n. 2016/679 del 27/4/2016 in materia di tutela e conservazione dei dati personali degli interessati al trattamento. Le azioni e le misure per il trattamento dei dati personali in condizione di sicurezza con la finalità di ridurre al minimo, con riferimento alla tipologia di dati trattati, i rischi di distruzione o perdita degli stessi, nonché i rischi di accesso non autorizzato, il trattamento non consentito o non conforme alle finalità di raccolta.

Si procede, quindi, all'analisi dei seguenti elementi:

1. elenco dei trattamenti di dati personali;
2. distribuzione dei compiti e delle responsabilità nell'ambito della struttura preposta al trattamento dei dati;
3. analisi dei rischi a cui sono soggetti i dati;
4. misure adottate e da adottare per garantire l'integrità e la disponibilità dei dati e la protezione delle aree e dei locali;
5. criteri e modalità di ripristino dei dati a seguito di distruzione o danneggiamento;
6. pianificazione degli interventi formativi previsti.

## **DESCRIZIONE DELL'ATTIVITÀ**

L'attività oggetto del mandato professionale/del contratto di fornitura di servizi contabili e amministrativi consiste:

- > Nell'elaborazione della contabilità e delle dichiarazioni fiscali dei propri clienti.
- > .....

## **SEDE ED UNITA' LOCALI**

da inserire

## **TIPOLOGIA DEI DATI TRATTATI**

L'attività esercitata e descritta in premessa comporta la raccolta e la gestione di dati personali, come di seguito indicati:

- a) fatture e corrispondenza della propria clientela, con indicazione sulle stesse dei dati fiscali e civilistici obbligatori per legge volti ad individuare i soggetti fra i quali è intercorso un rapporto giuridico o economico;
- b) estratti conto bancari o postali e relativa documentazione collegata, quali le matrici di assegni, le ricevute di deposito di valori, le ricevute bancarie di pagamento o incasso, le cambiali e gli altri titoli di credito o documenti attinenti i rapporti con gli istituti di credito e le Poste Italiane S.p.A.;

- c) polizze di assicurazione relative ai rischi aziendali o personali dei clienti per i quali si gestiscono gli aspetti contabili e dichiarativi;
- d) dichiarazioni fiscali obbligatorie, nelle quali sono altresì indicati i dati anagrafici e parentali del titolare della dichiarazione e dei suoi familiari. È altresì indicato nella dichiarazione dei redditi l'eventuale opzione per il versamento dell'8% alla comunità religiosa indicata dal cliente;
- e) ricevute relative alle spese mediche, farmaceutiche e simili relative al cliente ed ai suoi familiari, fornite per la compilazione della dichiarazione dei redditi;
- f) copie di atti di proprietà, mutuo, costitutivi e modificativi di società e di modifica dei rapporti di matrimonio dei clienti dello studio;
- g) copia di documenti di identità necessari per la comunicazione agli Istituti ed Enti pubblici;
- h) copia di libretti di circolazione di veicoli in genere utili per la corretta redazione della contabilità e per la presentazione di comunicazioni fiscali ed amministrative ai vari Enti pubblici;
- i) modelli di pagamento delle imposte e dei contributi di ogni tipo e genere;
- j) visure e certificati della Camera di Commercio o del Catasto Terreni e Fabbricati.

In relazione alla sicurezza delle informazioni, il Titolare del Trattamento utilizza i dati personali o sensibili ricevuti dall'Interessato per l'espletamento dei seguenti compiti:

- > la redazione della contabilità;
- > la compilazione delle dichiarazioni fiscali in genere (redditi, ICI, IVA, IRAP, sostituti d'imposta, ecc.);
- > la compilazione di Studi di Settore, questionari, ecc.;
- > la compilazione di pratiche e modelli relativi alle CCIAA, Entri previdenziali e assistenziali, Albi, Ruoli ed Elenchi;
- > la compilazione di pratiche, modelli ed istanze relativi al rilascio o rinnovo di autorizzazioni amministrative e licenze rilasciate da qualsiasi Ente e autorità;
- > il pagamento di tutte le imposte a qualsiasi titolo e con qualsiasi mezzo (come ad esempio i contratti di locazione telematici e i modelli F24 on-line);
- > le pratiche al Contenzioso Tributario;
- > la consulenza aziendale e tributaria in genere.

## **STRUMENTI CON I QUALI SI EFFETTUANO I TRATTAMENTI E CAUTELE DA ADOTTARE**

Per l'esecuzione dell'attività, vengono utilizzati personal computer, server e software specifici.

I dati personali o sensibili che non sono stati inseriti negli applicativi, vengono conservati con modalità cartacea secondo le regole più sotto descritte.

Il personale dipendente ed i collaboratori dopo aver utilizzato i documenti cartacei li inseriscono negli appositi faldoni e li depongono negli appositi armadi, avendo cura di chiuderli in maniera da impedire a soggetti terzi l'accesso ai dati.

Il personale dipendente ed i collaboratori nell'utilizzo dei sistemi informatici in dotazione hanno cura di lasciare incustodita la propria postazione di lavoro per il minor tempo possibile.

Qualora il personale dipendente ed i collaboratori ritenessero di dover lasciare incustodita la propria postazione di lavoro, dovranno provvedere a riporre i documenti cartacei negli appositi armadi ed a spegnere il terminale Hardware affidatogli.

Eventuali copie di documenti, di scritti, di appunti, di tabulati di prova, ecc. vengono distrutti al termine del loro utilizzo in maniera tale da renderli incomprensibili, anche tramite macinatura.

E' fatto espresso divieto di utilizzare carta riciclata per stampare documenti da consegnare a terzi.

## **SCHEDARI ED ALTRI SUPPORTI**

Le fatture ed i documenti relativi agli incassi e pagamenti vengono tenuti presso lo Studio per il tempo necessario per adempiere agli obblighi di legge e successivamente restituiti al cliente per la loro conservazione. Sono conservati, nel periodo di giacenza presso la struttura, in appositi contenitori intestati ad ogni singolo cliente e depositi, dopo l'uso, in armadi che a fine giornata lavorativa sono chiusi a chiave.

I libri contabili, depositati presso il Titolare del Trattamento, sono tenuti in appositi raccoglitori intestati ad ogni cliente. Tali raccoglitori, sono riposti in appositi armadi muniti di serratura che a fine giornata lavorativa sono chiusi a chiave.

Le dichiarazioni fiscali ed i relativi allegati (oneri deducibili, modelli di versamento delle imposte, ecc.), sono conservati anch'essi in contenitori intestati ad ogni cliente ed archiviati in appositi armadi muniti di serratura e chiusi a chiave alla fine di ogni giornata lavorativa.

Tutte le chiavi sono depositate in luogo sicuro ed accessibile esclusivamente al Titolare del trattamento o agli Incaricati al trattamento.

## **DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITÀ**

Il titolare del trattamento è l'unico responsabile della protezione dei dati, salvo la nomina di uno o più responsabili del trattamento.

La nomina di eventuali Responsabili al trattamento è effettuata in forma scritta.

Il Titolare del trattamento dei dati ha nominato mediante incarico formale gli Incaricati del trattamento dei dati.

Gli incaricati al trattamento dovranno trattare i dati di ogni singolo Interessato avendo cura che dalla propria scrivania siano stati rimossi ed archiviati tutti i dati personali del precedente Interessato (Cliente).

Gli incaricati al trattamento dovranno aver cura di conservare i dati contabili distintamente dai dati relativi alle dichiarazioni di ogni singolo Interessato (Cliente).

Gli incaricati al trattamento dovranno aver cura di conservare i dati sensibili di ogni Interessato (Cliente) in busta chiusa che andrà sigillata dopo ogni utilizzo dei dati stessi e riposta negli appositi archivi.

Oltre alle istruzioni generali appena esposte sulle modalità operative per il trattamento dei dati personali, ad ogni singolo incaricato, oltre alle mansioni assegnate, sono state illustrate:

- > le modalità di utilizzo e custodia della password utili all'accesso ai personal computer;
- > le modalità di utilizzo e custodia delle chiavi di ogni singolo armadio o classificatore;
- > le modalità e le procedure per proteggere i sistemi informativi;
- > le modalità di utilizzo e protezione di supporti rimovibili;
- > le procedure per il salvataggio di dati.

Il Titolare del trattamento può condividere i dati dei propri clienti con uno o più Contitolari al trattamento. La contitolarità del trattamento avviene esclusivamente in forma scritta.

Il Titolare del trattamento si avvale, per lo svolgimento dell'incarico ricevuto dall'Interessato di una struttura esterna. Con tale struttura è stato redatto un apposito e puntuale contratto nel quale sono stati indicate tutte le regole comportamentali che tale struttura esterna dovrà osservare nello svolgimento del contratto; contratto al quale si rimanda.

## **SOGGETTI INCARICATI DELLA GESTIONE E MANUTENZIONE DEL SISTEMA**

Il supporto tecnico per la manutenzione degli strumenti elettronici viene svolto dalla ditta :

.....

Il supporto tecnico per la manutenzione dei software utilizzati per il trattamento dei dati viene svolto dalla ditta :

....

Ai soggetti incaricati della gestione e manutenzione del sistema informativo, siano essi interni o esterni all'organizzazione del Titolare, viene prescritto di non effettuare alcun trattamento, sui dati personali contenuti negli strumenti elettronici, fatta unicamente eccezione per i trattamenti di carattere temporaneo strettamente necessari per effettuare la gestione o manutenzione del sistema.

Le lettere ed i contratti di nomina dei responsabili, le lettere di incarico o di designazione degli incaricati vengono raccolte in modo ordinato, in base alla unità organizzativa cui i soggetti appartengono: in tale modo il Titolare dispone di un quadro chiaro di chi fa cosa (mansionario privacy ), nell'ambito del trattamento dei dati personali.

Periodicamente, con cadenza almeno annuale, si procede ad aggiornare la definizione dei dati cui gli incaricati sono autorizzati ad accedere, e dei trattamenti che sono autorizzati a porre in essere, al fine di verificare la sussistenza delle condizioni che giustificano tali autorizzazioni.

La stessa operazione viene compiuta per le autorizzazioni rilasciate ai soggetti incaricati della gestione o manutenzione degli strumenti elettronici.

### **ANALISI DEI RISCHI CHE INCOMBONO SUI DATI E MISURE IN ESSERE**

L'analisi dei possibili rischi che gravano sui dati è stata effettuata in relazione alla causa che può generare il rischio e quindi classificati in:

- rischi legati ai comportamenti degli Incaricati del trattamento dei dati;
- rischi legati agli strumenti utilizzati per il trattamento dei dati;
- rischi legati al contesto ambientale in cui avviene il trattamento dei dati.

Nella tabelle seguenti, per ogni tipologia di rischio, si indicano gli eventi che potrebbero verificarsi e quindi mettere a rischio l'integrità dei dati trattati. Si evidenzia, inoltre, la gravità di ogni rischio.

<b>Comportamenti degli Incaricati al trattamento dei dati</b>	<b>RISCHIO</b>	<b>Descrizione dell'impatto sulla sicurezza</b>
	Perdita del lavoro in fase di esecuzione	
	Cancellazione di dati importanti dai supporti di memorizzazione	
	Danneggiamento delle apparecchiature	
	Sottrazione o perdita delle password o chiavi degli armadi o classificatori	

L'analisi appena descritta è stata effettuata in quanto può accadere che in fase di lavoro avvenga la perdita di dati per disattenzioni o simili. Il livello appare basso in quanto:

- > il personale incaricato dispone di tutte le conoscenze necessarie al trattamento dei dati;

- > il personale incaricato dispone di buone conoscenze degli strumenti informatici utilizzati;
- > ogni postazione di lavoro dispone di una password personale dell'utente. L'incaricato è stato istruito sulle modalità di creazione di una password complessa;
- > tutti i dati inseriti sono ricostruibili mediante le copie di back-up che vengono effettuate giornalmente/settimanalmente.

Comportamenti degli Incaricati al trattamento dei dati	RISCHIO	Descrizione dell'impatto sulla sicurezza
	Accessi esterni non autorizzati	
	Presenza di virus informatici o programmi che possono arrecare danno	
	Spamming o tecniche di sabotaggio	
	Malfunzionamento, indisponibilità, guasti o degrado degli strumenti	
	Sottrazione di dati da parte degli incaricati	

L'analisi appena descritta è stata effettuata in quanto può accadere che durante la navigazione in rete ci possano essere infiltrazioni di virus informatici o malfunzionamento degli strumenti. Il livello appare basso in quanto:

- > i personal computer si trovano all'interno di una rete protetta da firewall;
- > tutti i personal computer sono dotati di antivirus aggiornato periodicamente o aggiornato automaticamente;
- > non si sono finora mai registrati guasti o malfunzionamenti rilevanti all'interno dello Studio;
- > tutti i personal computer sono collegati ad un gruppo di continuità che garantisce l'operatività dei personal computer per il tempo sufficiente alla chiusura di tutti i processi e programmi aperti e lo spegnimento degli stessi. I dati trattati sono conservati sul server che in caso di mancanza di corrente viene automaticamente spento dal gruppo di continuità stesso prima del totale esaurimento della batteria del gruppo stesso. Agli incaricati al trattamento sono state impartite istruzioni volte anche allo spegnimento della stazione di lavoro al termine della giornata lavorativa ed ogni qualvolta la postazione rimanesse incustodita per oltre un'ora.

Inoltre, i rischi appena analizzati, oltre che al rischio di danneggiamento per eventi atmosferici, risultano essere di basso impatto in quanto:

- > il locale archivio è accessibile solo previo prelievo delle chiavi di chiusura dello stesso contenute nell'apposita custodia;
- > il locale archivio è dotato di scaffalature rialzate per evitare il pericolo di allagamenti;

- > tutti i personal computer sono rialzati da terra al fine di evitare contatti immediati con l'acqua e per la riduzione dell'introduzione di polveri nello stesso;
- > periodicamente si procede alla rimozione delle polveri all'interno dei personal compute, tramite ditta specializzata di assistenza hardware;
- > il personale addetto alla pulizia dei locali è stato informato della modalità di accesso e di esecuzione dei lavori nei locali mediante apposito contratto; detto personale è l'unico autorizzato all'accesso al di fuori dell'orario di lavoro; al personale stesso sono state fornite le chiavi di accesso ai locali, ma non è stata loro reso noto il luogo di conservazione delle chiavi degli armadi e mobili in genere dove sono conservati i documenti; all'impresa di pulizie viene inoltre richiesta la massima cautela nella selezione del personale da inviare presso la sede del trattamento dei dati;
- > gli inquilini del condominio non hanno in alcun modo accesso ai locali;
- > tutto il materiale cartaceo, al termine della giornata lavorativa, viene riposto negli armadi o classificatori e chiusi a chiave;
- > la struttura dispone di estintori antincendio;
- > l'accesso alla struttura è protetto da porte blindate con serratura antiscasso e le finestre da inferriate;
- > la struttura è dotata di impianto di allarme.

### **CRITERI E PROCEDURE PER IL RIPRISTINO DELLA DISPONIBILITÀ DEI DATI**

Sono previste delle procedure di salvataggio dei dati grazie alle quali si può procedere al ripristino in caso di perdita o danneggiamento degli stessi in tempi brevi.

#### **Ripristino**

<b>Banca / data base / archivio di dati</b>	<b>Criteria e procedure per il salvataggio e il ripristino dei dati</b>	<b>Pianificazione delle prove di ripristino</b>
Banca dati del server	Back-up giornaliero	A cura del Titolare del Trattamento
Archivi dati in ogni personal computer	Back-up periodico	A cura del Titolare del Trattamento

#### **Salvataggio**

<b>Banca / data base / archivio di dati</b>	<b>Criteria e procedure per il salvataggio</b>	<b>Luogo di custodia delle copie di sicurezza</b>	<b>Persona incaricata del salvataggio</b>
Banca dati del server	Back-up giornaliero	Le copie vengono custodite nella cassaforte	A cura del Titolare del Trattamento
Archivi dati in ogni personal computer	Back-up periodico	Le copie vengono custodite nella cassaforte	A cura del Titolare del Trattamento

### **PIANIFICAZIONE DEGLI INTERVENTI FORMATIVI PREVISTI**

In ossequio al disposto normativo di cui al Regolamento UE n. 2016/679 del 27/4/2016, il Titolare del Trattamento promuove e programma periodiche attività di formazione e di aggiornamento per gli incaricati del trattamento dei dati personali avvalendosi di figure professionali interne od esterne. Il piano formativo viene programmato ogni qualvolta si renda necessario sia per un ripasso delle regole previste che a seguito di modifiche normative intervenute ed in tutti i casi di aggiornamento degli strumenti informatici.

Ad ogni nuovo incaricato del trattamento dei dati professionali vengono fornite tutte le istruzioni per un corretto trattamento dei dati personali e sensibili.

Al momento dell'assegnazione di un personal computer vengono assegnate le credenziali di autenticazione ed eventualmente armadi o quanto altro utile per una corretta conservazione dei dati.

Saranno illustrate le tecniche e le procedure già in essere presso lo Studio per un corretto trattamento dei dati.

Al nuovo incaricato del trattamento dei dati viene fatta conoscere la struttura e le modalità di accesso agli archivi.

### CONCLUSIONI

Il titolare del Trattamento ha impostato un sistema efficiente di sicurezza delle informazioni atto a ridurre le probabilità che si verifichino danni di qualsiasi tipo ai dati trattati.

Il Titolare del Trattamento, attraverso la valutazione dei rischi, si propone di far fronte ad ogni minaccia ai propri dati con le misure di sicurezza più adeguate, stanziando quando e dove richiesto, risorse per la migrazione dei propri strumenti elettronici e di tutti i beni (armadi, cassettiere, ecc) preposti alla protezione dei dati.

Il Titolare del Trattamento, oltre ad un'attività formativa del personale dipendente e dei collaboratori esegue continui controlli sugli stessi affinché svolgano le rispettive mansioni nel rispetto delle norme e delle direttive emanate dal Titolare stesso.

La presente analisi e valutazione dei rischi connessi al trattamento dei dati è stata effettuata al fine della verifica che la struttura rispetti le previsioni del Regolamento UE n. 2016/679 più volte citato.

ALGHERO , li

14/03/2019

Il Titolare del trattamento  
