POLICY PER IL GOVERNO DEI RISCHI DI VIOLAZIONE DEI DATI PERSONALI GDPR 679/2016

CGF s.r.l
Via G. Paisiello, 19
80128 Napoli (NA)
P.IVA 05364431212
Fax (+39) 081 0098951
Tel (+39) 08119090880
info@cgfsrl.eu
direzione@cgfsrl.eu

INDICE

Sommario

1. REMESSA

CGF SRL (di seguito "società"), al fine di dimostrare che il trattamento dei dati personali è effettuato in conformità al Regolamento UE 2016/679 (General Data Protection Regulation - di seguito per brevità "GDPR"), ha predisposto il presente documento denominato "Policy GDPR".

Questo documento è approvato ed aggiornato dalla Direzione e dal personale aziendale individuato, con l'ausilio ed il supporto del Responsabile della Protezione dei dati personali (RPD).

Il presente manuale rappresenta lo strumento operativo e gestionale per programmare e verificare l'adozione delle misure tecniche e organizzative adeguate, secondo quanto previsto dagli articoli 24 e 32 del GDPR.

Il Manuale GDPR, pertanto, costituisce un valido strumento per:

- definire compiti, istruzioni e responsabilità dei soggetti, che a vario titolo sono preposti al trattamento dei dati personali e all'adozione delle misure tecniche ed organizzative di sicurezza e di protezione;
- descrivere le politiche aziendali, nonché le azioni e gli adempimenti adottati per garantire un livello di sicurezza adeguato;
- individuare indirizzi e misure per consentire la gestione delle emergenze e garantire la continuità operativa ed il ripristino degli strumenti e dei dati;
- indicare azioni per consentire il controllo del sistema di sicurezza.

Il presente manuale è strutturato in paragrafi e allegati:

1. i paragrafi recano la descrizione delle azioni da adottare e delle regole generali da rispettare, per cui sono conoscibili da tutti;
2. gli allegati contengono le indicazioni operative e la descrizione delle misure tecniche ed organizzative adottate dalla società (per cui di norma non sono pubblici, in quanto aventi natura riservata e riferita a processi critici).

CGF s.r.l
Via G. Paisiello, 19
80128 Napoli (NA)
P.IVA 05364431212
Fax (+39) 081 0098951
Tel (+39) 08119090880
info@cgfsrl.eu
direzione@cgfsrl.eu

2. PROFILI SOGGETTIVI

2.1 Titolare e Responsabili del Trattamento

La disciplina europea in tema di protezione dei dati personali (GDPR), in continuità rispetto al codice della privacy italiano, individua due figure soggettive particolari, aventi una responsabilità specifica per quanto concerne il trattamento dei dati personali:

a) il titolare del trattamento: è CGF SRL (di seguito per brevità "società"), come entità considerata nel suo complesso, rappresentata dall'amministratore delegato o dall'Amministratore Unico;

b) il responsabile del trattamento (art. 28 GDPR): è la persona fisica o la persona giuridica che presenta garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del regolamento e garantisca la tutela dei diritti dell'interessato.

I responsabili del trattamento possono essere individuati sia all'interno dell'organizzazione aziendale (quindi, nella figura di dipendenti della società), sia all'esterno, nelle figure che, in base ad un contratto o ad un atto, prestano servizi per conto della società e quindi sono preposte a svolgere operazioni di trattamento in nome e nell'interesse della stessa.

In tal caso, la società predispone ed aggiorna un elenco di tutti i fornitori, consulenti e collaboratori esterni, ai quali sono affidati attività e compiti che comportano la necessità di accedere agli strumenti elettronici aziendali e quindi ai dati personali, per cui occorre formalizzare la designazione in qualità di responsabile del trattamento.

Ai soggetti esterni possono essere affidati sia compiti di natura operativa (concernenti le operazioni di trattamento), sia funzioni di gestione degli strumenti con profili di accesso privilegiati, per cui sono assegnate funzioni di amministrazione di sistema.

A ciascun soggetto, indicato nella procedura **Pr02** e relativi allegati atti di nomina, è quindi conferita la qualità di:

1 Responsabile del trattamento, utilizzando la apposita lettera di nomina, predisposta ai sensi dell'art. 28 del GDPR;

2. Amministratore di Sistema utilizzando la apposita lettera di nomina, predisposta ai sensi degli art. 28-32 del GDPR;

Quindi, ai responsabili sono affidati i compiti e le funzioni indicate come da allegati alla procedura richiamata, comprese, ove necessario, anche quelle relative all'amministrazione dei sistemi;

2.2 Autorizzati al trattamento di dati personali

Il titolare o il responsabile del trattamento svolge le operazioni di trattamento mediante la preposizione e l'ausilio di persone fisiche: si tratta dei soggetti autorizzati al trattamento (ai sensi dell'art. 29 GDPR), che, in continuità rispetto al codice della privacy, possono continuare ad essere chiamati incaricati del trattamento.

Secondo la definizione riportata nel GDPR si tratta di "chiunque agisca sotto l'autorità del titolare o del responsabile del trattamento, dovendo essere istruito con un atto scritto".

Gli autorizzati al trattamento possono essere sia soggetti interni all' organizzazione aziendale, sia soggetti esterni, che operano autonomamente oppure all'interno di una organizzazione.

La designazione degli autorizzati al trattamento (alias incaricati del trattamento) è effettuata dal responsabile del trattamento ed avviene mediante una apposita lettera, il cui formato generale è riportato nella procedura per la nomina **Pr 02 richiamata in precedenza**.

2.3 Responsabile della protezione dei dati

Ai soggetti indicati nei due paragrafi precedenti, con l'adozione del GDPR si aggiunge il Responsabile della protezione dei dati (RPD), che è figura obbligatoria quando il trattamento dei dati è effettuato da un'autorità pubblica ovvero nelle ipotesi previste dall'art. 37 del Regolamento UE 2016/679.

La società, ancorché non obbligata, ha scelto di procedere alla nomina di un RPD, al fine di avere una figura, cui affidare i compiti di consulenza a favore del titolare e dei responsabili e di sorveglianza dell'osservanza del GDPR.

A tal fine, è stato designato un esperto in materia di data protection, al quale sono stati affidati i compiti riportati nella lettera di nomina nella procedura per la nomina del RPD **PR03**.

3. ELENCO DEI DATI OGGETTO DI TRATTAMENTO

Il Regolamento UE 2016/679 (GDPR) ha ad oggetto la disciplina dell'attività di trattamento dei dati personali. In particolare:

- per trattamento si intende "qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insieme di dati personali, con la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento, o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione" ;
- per dato personale si intende "qualsiasi informazione riguardante una persona fisica identificata o identificabile (''interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale".

Dall'esame delle definizioni si evince che il GDPR si applica solo ed esclusivamente ai trattamenti di dati personali riferiti a persone fisiche, mentre sono escluse dall'ambito di applicazione del regolamento le informazioni relative alle persone giuridiche.

Sono due le categorie fondamentali di dati personali:

- dati particolari: si intendono i dati che "rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona";
- dati comuni: le informazioni riferite a persone fisiche identificate o comunque identificabili, che non siano idonee a rivelare gli stati, i fatti e le qualità, di cui all'art. 9 del GDPR, per i quali è vietato il trattamento, salvo che non ricorrano i presupposti di liceità e di legittimazione, previsti dal comma 2 dell'articolo ivi considerato.

La società tratta sia dati comuni che dati particolari con riferimento ai dati giudiziari stante la necessità della vigilanza dovuta per il mantenimento dei requisiti per l'iscrizione nelle white list e per il conseguimento e mantenimento del rating di legalità. Il trattamento è comunque inteso nell'ambito di quanto consentito ai sensi della legge 300/70 art.8.

Comunque in tal senso oltre al rifermento del contratto collettivo l'azienda si avvale di una specifica autorizzazione all'acquisizione e uno specifico strumento di archiviazione della documentazione comprovante lo status giudiziario del dipendente.

La società, al fine di gestire correttamente le operazioni di trattamento e di dimostrare che il trattamento è effettuato conformemente al Regolamento UE 2016/679, predispone ed aggiorna un elenco degli strumenti elettronici e dei sistemi informatici in uso per il trattamento dei dati personali o comunque considerati critici per i processi aziendali, al fine di avere una mappatura degli strumenti da proteggere. Inoltre, nel medesimo allegato, unitamente agli strumenti e ai sistemi, è riportato un elenco dei trattamenti di dati personali, costituente la base per l'analisi e la valutazione dei rischi e per il conferimento degli incarichi e la formalizzazione delle autorizzazioni e delle istruzioni.

L'elenco degli strumenti e dei sistemi, nonché dei trattamenti di dati societari è riportato nel registro del trattamento oggetto di specifica procedura comprensivo di allegati **PR01.**

4. ISTRUZIONI PER IL TRATTAMENTO E PROTEZIONE DEI DATI PERSONALI - STRUMENTI

4.1 Obiettivi in materia di sicurezza e modalità del trattamento dei dati

Gli obiettivi di sicurezza, che la società si pone con la redazione e l'aggiornamento del presente manuale, sono:

1. dimostrare che sono adottate le misure tecniche ed organizzative adeguate, secondo quanto previsto dall'art. 24 del GDPR;
2. garantire il rispetto del principio della privacy by design, ai sensi dell'art. 25, comma 1 del GDPR;
3. mettere in atto le misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento (privacy by default), ai sensi dell'art. 25, comma 2 del GDPR;
4. ridurre, a livelli accettabili e gestibili, i principali rischi di sicurezza, a cui il sistema informativo aziendale può essere sottoposto;
5. mantenere, compatibilmente con i vincoli di sicurezza previsti dal GDPR e dalle eventuali indicazioni dell'Autorità Nazionale di Controllo, il massimo livello di usabilità del sistema.

4.2 Principi generali in materia di conservazione dei dati e delle informazioni

La società, in qualità cli titolare del trattamento, provvede a determinare le finalità e le modalità dei trattamenti.

Pertanto, al fine di garantire la conformità delle attività di trattamento dei dati al GDPR, la società procede a:

- nominare soggetti interni all'organizzazione aziendale (elencati in PR02) in qualità di responsabili del trattamento, utilizzando il modello di atto di nomina riportato in allegato **(PR02);**
- designare in qualità di responsabili del trattamento gli autorizzati al trattamento (ossia incaricati al trattamento dei dati ossia le persone fisiche preposte allo svolgimento delle operazioni di trattamento, utilizzando l'apposita lettera **PR02**);
- inviare per posta elettronica (all'indirizzo individuale assegnato dall'azienda o a quello dichiarato all'atto della sottoscrizione del contratto cli collaborazione) a ciascuna persona (sia dipendente, sia collaboratore strutturato) le istruzioni scritte per il trattamento dei dati **(riportate nell'allegato PR02)**;
- **identificare la definizione del profilo di autorizzazione da associare alle credenziali di autenticazione assegnate a ciascun incaricato del trattamento dei dati. Per profilo cli autorizzazione si intende "l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti"; il "sistema di autorizzazione" è costituito dall'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente;**
- provvedere a richiedere la disattivazione, ovvero la variazione del profilo di autorizzazione associato a ciascun incaricato, nel caso in cui la persona fisica cessi di operare all'interno della struttura di propria competenza ovvero, per qualsiasi motivo, fosse stato modificato il suo profilo professionale;
- vigilare sull'attività svolta dagli incaricati del trattamento, verificando il rispetto delle procedure operative e delle istruzioni impartite dall'azienda, anche in materia di misure di sicurezza.

La società, inoltre, per quanto riguarda la gestione e la manutenzione degli strumenti elettronici, si avvale di soggetti esterni, che sono nominati dall' amministratore di sistema, in conformità alle indicazioni fomite dal Garante per la protezione dei dati personali nel provvedimento generale del 27 novembre 2008, così come modificato ed integrato con deliberazione del 25 giugno 2009.

La designazione delle persone fisiche in qualità di amministratore di sistema avviene mediante l'utilizzo del modello di lettera di nomina riportata in procedura **PR02**, che deve essere consegnata personalmente ovvero trasmessa a mezzo PEC alla persona o al consulente da nominare in qualità di amministratore di sistema o di responsabile esterno del trattamento, con funzioni di amministrazione di sistema.
Quest'ultimo è obbligato a sua volta a procedere alla designazione formale in qualità di amministratore di sistema delle persone fisiche, preposte allo svolgimento dei compiti di amministrazione di sistema, nell'interesse e per conto dell'azienda, in qualità di titolare.

4.3 Liceità del trattamento e obblighi di informazione

Il trattamento dei dati personali deve essere svolto in modo lecito, corretto e trasparente, secondo quanto previsto dall'art. 5 del GDPR.

Inoltre, la raccolta dei dati deve avvenire per finalità determinate, esplicite e legittime e i dati possono essere trattati in modo che l'attività da svolgere non sia incompatibile con tali finalità.
Pertanto, all'interessato o alla persona che fornisce i dati, al momento della raccolta degli stessi, deve essere fornita una idonea informativa, nelle forme previste dagli articoli 12 – 13 – 14 del GDPR.
A tal fine, la società ha predisposto un formulario, contenente le diverse informative da utilizzare per tale adempimento.
Oltre, all'obbligo di informativa, affinché il trattamento dei dati sia lecito, occorre che siano rispettate le regole di legittimazione, previste rispettivamente per la raccolta ed il trattamento dei dati comuni e dei dati particolari dagli articoli 6 e 9 del GDPR.

Per quanto concerne i trattamenti di dati personali di cui è titolare la società di norma non occorre l'acquisizione del consenso dell'interessato, considerato che le finalità del trattamento medesimo sono connesse all'adempimento o all'esecuzione di prestazioni di un contratto di cui è parte l'interessato medesimo ovvero per adempiere un obbligo legale.

La modulistica da utilizzare per adempiere all'obbligo di informativa e all'eventuale raccolta del consenso da parte dell'incaricato (ove necessario) è riportata in procedura **PR04.**

5. SICUREZZA DEI DATI PERSONALI: PRINCIPI

L'art. 32 del GDPR prevede che "tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio".

La sicurezza può essere definita come "l'insieme delle misure atte a garantire la disponibilità, l'integrità e la riservatezza delle informazioni gestite" e dunque "l'insieme di tutte le misure atte a difendere il sistema informativo dalle possibili minacce d'attacco".

I rischi di perdita dei dati, anche accidentale, di accesso abusivo e di trattamento illecito o non consentito dei dati possono essere causati (a titolo meramente esemplificativo) da:

- malfunzionamenti di sistemi hardware e software, applicativi software e servizi;
- persone esterne all'organizzazione (hacker, spie, terroristi, vandali, ecc.);
- eventi naturali (inondazioni, incendi, terremoti, tempeste, ecc.);
- persone interne all'organizzazione.

Tali rischi possono essere identificati come:

- accidentali,
- deliberati.

Rendere sicuro un sistema informatico non significa esclusivamente attivare un insieme di contromisure specifiche, di carattere tecnologico ed organizzativo, che neutralizzino tutti gli attacchi ipotizzabili al sistema di servizi, ma comporta l'esigenza di collocare ciascuna delle contromisure individuate in una politica organica di sicurezza, che tenga conto dei vincoli (tecnici, logistici, organizzativi, amministrativi e legislativi) imposti dalla struttura tecnica ed organizzativa, in cui la società opera e che giustifichi ciascuna contromisura in un quadro complessivo.

Principale obiettivo di un sistema di sicurezza è quindi la salvaguardia delle informazioni.

A tal fine, per ciascun sistema informativo automatizzato aziendale, per gli strumenti elettronici e per gli archivi e documenti cartacei deve essere fornita la cosiddetta garanzia "R.I.D.", ossia "Riservatezza – Integrità – Disponibilità".

Di seguito, per completezza, si riportano le definizioni di ciascuna garanzia:

- Riservatezza (o Confidenzialità): solo gli utenti autorizzati possono accedere alle informazioni necessarie;
- Integrità: protezione contro alterazioni o danneggiamenti; tutela dell'accuratezza e completezza dei dati;
- Disponibilità: le informazioni sono rese disponibili quando occorre e nell'ambito di un contesto pertinente.

Fra le risorse (asset) da tutelare rientrano certamente:

- dati digitali;
- documenti cartacei;
- flussi informativi;

nonché componenti materiali come:

- server;
- computer;
- reti;
- il personale;
- gli edifici;
- gli uffici.

L'approccio alla sicurezza deve avvenire in una logica di prevenzione (ossia mediante l'utilizzo di metodologie e di strumenti di risk management) piuttosto che in una logica di gestione delle emergenze o di semplice controllo / vigilanza.

L'architettura del sistema, al fine di garantire le esigenze di sicurezza di protezione degli strumenti e dei dati, si basa su 3 elementi fondamentali:

- le politiche aziendali di sicurezza;
- le soluzioni organizzative e tecnologiche;
- gli atteggiamenti individuali.

Un sistema di gestione della sicurezza delle informazioni efficiente ed efficace permette all'organizzazione di:

- mantenersi aggiornata su nuove minacce e vulnerabilità e prendere le medesime in considerazione in modo sistematico;
- trattare incidenti e perdite in ottica di prevenzione e di miglioramento continuo del sistema;
- sapere in tempo utile quando politiche di sicurezza e procedure non sono implementate, per prevenire potenziali danni;
- implementare politiche e procedure di primaria importanza.

Le misure tecniche ed organizzative devono essere adottate mediante l'utilizzo di un processo di autodeterminazione, per cui occorre provvedere alla riduzione dei rischi, che possono interessare i dati personali oggetto di trattamento in seno all'azienda e che riguardano il sistema informativo nel suo complesso.

Il sistema di protezione dei dati personali della società si basa sui seguenti principi generali:

- tutte le informazioni (dati, documenti, archivi, …) devono essere protette e disponibili;
- al fine di garantire la riservatezza dei contenuti e delle informazioni, la sicurezza deve riguardare anche le reti di comunicazioni elettroniche dei dati;
- si deve procedere alla previsione di misure di sicurezza per la protezione di aree e locali, in cui sono localizzati i server, considerati "sensibili" per l'attività dell'azienda, e gli archivi cartacei, monitorandone le caratteristiche tecniche e le misure di tutela dagli accessi non autorizzati;
- tutte le operazioni di trattamento dei dati, effettuate utilizzando strumenti connessi alla rete di comunicazione elettronica, devono essere oggetto di tracciabilità, garantendo il non ripudio delle operazioni svolte, dovendo utilizzare un sistema di autenticazione informatica, che consenta un controllo dell'identità di "chi sta facendo che cosa";
- devono essere predisposte misure tecniche ed organizzative di sicurezza per l'accesso ai locali, che ospitano i server e gli strumenti elettronici in dotazione, favorendo possibilmente la localizzazione e l'ubicazione in unico luogo o in luoghi collegati, al fine di consentire una migliore gestione degli strumenti e della sicurezza attiva e passiva;
- ogni eventuale incidente o evento straordinario, che possa pregiudicare la sicurezza dei dati e dei sistemi, deve essere oggetto di analisi e di rapporto scritto;

- tutti i progetti per lo sviluppo di nuovi sistemi / servizi, aventi natura trasversale e che possano interessare il sistema informativo dell'azienda, devono essere comunque gestiti secondo quanto riportato nel presente manuale;
- al pari, tutte le modifiche eventualmente apportate ai processi organizzativi devono essere documentate nel presente manuale o nei documenti del sistema di qualità aziendale.

Sotto il profilo della data protection, con l'espressione "continuità operativa" si intende "l'insieme di attività volte a ripristinare lo stato del sistema informatico o parte di esso, compresi gli aspetti fisici e organizzativi e le persone necessarie per il suo funzionamento, con l'obiettivo di riportarlo alle condizioni antecedenti a un evento disastroso".

Al fine di garantire la continuità operativa dei sistemi e quindi dei trattamenti di dati personali, nonché allo scopo di fronteggiare eventi che possano causare il danneggiamento degli strumenti elettronici e la distruzione o perdita delle informazioni cd. critiche, si devono prevedere azioni per fronteggiare l'emergenza e le possibili interruzioni dei processi produttivi.

Per far fronte a tali esigenze di conservazione dei dati, accesso e recupero la Società ha affidato la gestione della struttura informatica all'esterno, ad un'Azienda con notevole expertise in termini di gestione delle reti e apparecchiatura informatica (server).

Nomina un amministratore di sistema che assicura, attraverso il supporto della menzionata società, i livelli sufficienti di sicurezza del sistema informativo nel suo complesso.

In merito all'accesso fisico agli apparati questo è consentito solo all'amministratore di sistema o al suo delegato in sua assenza.

In tabella si riporta il framework privacy della società.

Documento	Descrizione	Ultima Revisione	Causali aggiornamento	Destinatari	Modalità distribuzione
PR01	Elenco degli strumenti elettronici e dei trattamenti dei dati personali: **Registro del Trattamento (allegati sistemi informativi)**	__/__/____	Prima redazione	Documento riservato	Documento interno
PR02	Procedura di Nomina Responsabile del trattamento, Amministratore di sistema, Incaricati al trattamento	__/__/____	Prima redazione	Documento riservato	Documento interno
PR03	Designazione responsabile della protezione dei dati personali	__/__/____	Prima redazione	Responsabile Protezione Dati (RPD)	Invio tramite PEC al soggetto individuato
PR04.01	Formulario informative e modulistica per consenso	__/__/____	Prima redazione	Clienti, Fornitori, Dipendenti, collaboratori, lavoratori	Inserire informativa su bolle, fatture, mail Consegna a ciascun dipendente o collaboratore all'atto dell'assunzione o della sottoscrizione del contratto Raccolta del consenso, ove necessario, mediante sottoscrizione di una copia del modulo
PR04.02		__/__/____	Prima redazione		
PR04.03		__/__/____	Prima redazione		
PR05	Procedura gestione Istanze e data breach	__/__/____	Prima redazione	Documento pubblico	Inserire come informativa nell'area privacy intranet e/o sito