PRIVACY DATA GOVERNANCE

IT Security Policy e privacy e sicurezza dei dati e delle informazioni

Le professioniste e i professionisti del mondo SCM Group trattano un significativo quantitativo di informazioni e dati personali dei propri dipendenti, clienti e terze parti. L'essenza stessa del lavoro del Gruppo consiste nel trattare dati di natura normativa, contrattuale, di business e connessi alle aspettative dei clienti e pertanto la protezione dei dati è uno dei profili su cui l'attenzione del Gruppo si è concentrata per allinearsi agli standard europei e internazionali.
La tutela dei dati rappresenta pertanto una priorità per il Gruppo nel mondo, declinato nell'ambito del proprio modello di *governance* e di *business*, in quanto può comportare ricadute positive per la salvaguardia del brand, la riduzione di perdite operative, la qualità delle relazioni con i clienti, il livello di fiducia con tutti i soggetti interessati e il rispetto degli obblighi normativi.

Il Gruppo ha adottato misure e accorgimenti di natura organizzativa e operativa volti alla protezione di qualsiasi soggetto che abbia rapporti con le *entities* del Gruppo. SCM Group ha, dunque, avviato un vasto programma di tutela dei dati personali che verranno riportati nelle seguenti sezioni, rappresentative dei tratti distintivi di tale programma.

1. Misure e accorgimenti di natura organizzativa e operativa volti alla protezione dei dati personali idonei a identificare gli interessati.

2. Misure e accorgimenti di natura tecnica IT Security Policy volti a mitigare i rischi che incombono sui dati personali trattati.

Data Protection Compliance Program

SCM Group si impegna a garantire la protezione dei dati personali trattati, attraverso un approccio basato sulla valutazione del rischio, insito in ogni trattamento, coerente con i requisiti normativi applicabili e con le aspettative dei dipendenti, clienti e terzi, nonché di tutti coloro che vengono in contatto a qualsiasi titolo col Gruppo.
SCM Group è attenta al miglioramento del sistema di protezione dei dati personali, al fine di soddisfare le istanze che arrivano dai clienti e le esigenze della normativa vigente, quali il Reg. UE 2016/679 in materia di protezione di dati personali e le linee guida dell'EDPB. In tale contesto, in un'ottica di rispetto del principio di *accountability*, il Gruppo ha provveduto a identificare e adottare adeguate misure tecniche e organizzative volte a rafforzare la protezione dei dati personali trattati e a mitigare gli eventuali rischi. Il Gruppo si è, altresì, dotato di un *Comitato Privacy*, nel quale vengono analizzate e risolte le problematiche che emergono dall'applicazione della disciplina normativa. Il programma *data protection* si articola a diversi livelli dell'organizzazione: a livello Global, a livello di Member Firm e a livello di singola country.

GDPR

Il Regolamento Generale sulla Protezione dei Dati, ufficialmente Regolamento n. 2016/679 e noto con la sigla "GDPR" (*General Data Protection Regulation*), entrato in vigore da aprile 2016 e diventato effettivo a partire dal 25 maggio 2018, ha apportato significativi cambiamenti alle norme riguardanti la protezione dei dati in Europa. Il Regolamento è finalizzato a uniformare le leggi riguardanti il trattamento e la protezione delle informazioni tra gli Stati Membri dell'Unione Europea, garantendo agli individui (tra cui, in particolare, tutti coloro che hanno rapporti con clienti e dipendenti del Gruppo) maggiori diritti di controllo sui propri dati personali.
La raccolta dati, la riservatezza e il rischio per la sicurezza sono temi trattate a livello globale e che SCM Group tiene tra le sue priorità.
I Paesi più evoluti nel mondo, caratterizzati da mercati multinazionali e dinamici, si sono dotati di strumenti, procedure e norme elevando il GDPR a «gold standard». Le organizzazioni sono

responsabili dell'adozione di adeguate misure di tutela dei dati personali sulla base dei rischi effettivi e attuali che incombono sui dati. Il Gruppo ha provveduto a definire e attuare un *Data Protection Compliance Program* in ragione delle molteplici aree che sono interessate dal Regolamento citato. Nel contesto di tale programma, sono state definite e implementate specifiche misure tecniche e organizzative atte a soddisfare i requisiti normativi applicabili e le obbligazioni dei clienti. Il Data Protection Compliance Program è mantenuto aggiornato per tener conto dell'evoluzione normativa e del contesto di *business*, dello scenario dei rischi e delle tecnologie emergenti. Le principali componenti del Data Protection Compliance Program di SCM Group sono:

• Registro delle attività di trattamento – il Gruppo ha mappato tutti i trattamenti, che coinvolgono i dati personali, in modo da distribuire correttamente ruoli e responsabilità, analizzare i rischi per i diritti e le libertà fondamentali degli interessati, sì da garantirne l'effettivo esercizio.

• Modello Organizzativo Data Protection – l'effettività delle misure di protezione dipende da un adeguato modello organizzativo dei ruoli preposti al governo delle operazioni svolte sui dati personali, dei ruoli di vigilanza (come il *Data Protection Officer*) e dei ruoli di garanzia. SCM Group mantiene aggiornato il proprio modello organizzativo di riferimento, ha nominato il *Data Protection Officer*, mantenendo un controllo capillare sui flussi dei dati personali circolanti nelle altre *legal entities*. Il Gruppo ha attivato una procedura di interlocuzione tra il nominato DPO e gli altri organi di vigilanza e controllo, valorizzando le diverse articolazioni dell'organigramma di compliance e istruendo la possibilità di verifiche capillari e diffuse.

• Informative sulla protezione dei dati – tutta la documentazione volta a garantire la trasparenza dei trattamenti svolti dal Gruppo è stata aggiornata per adeguarsi ai requisiti del GDPR, così da consentire piena tutela agli interessati e di avere piena contezza delle finalità, dei mezzi e basi giuridiche dei trattamenti effettuati, di ogni altra informazione necessaria, nonché di come esercitare i loro diritti.

• Clausole contrattuali con le terze parti – SCM Group ha definito e attuato adeguate clausole contrattuali con tutte le terze parti con cui ha relazioni di affari, sia all'interno che all'esterno dello spazio Europeo.

• Analisi di rischio e valutazione di impatto (DPIA) – SCM Group in Italia ha sviluppato e adottato una nuova analisi dei rischi e valutazione di impatto da applicare, anche a livello internazionale, ai trattamenti contenuti nel registro, al fine di indentificare ulteriori misure di tutela, in ragione dei potenziali danni materiali e immateriali che i trattamenti possono comportare per gli interessati.

• Politiche & Procedure – implementazione di nuove politiche e procedure sulla protezione dei dati, al fine di rispondere ai requisiti e agli standard definiti dal GDPR e da altre leggi in materia, tra cui:
– Politica generale di protezione dei dati: Privacy Data Governance;
– Procedura per la gestione delle violazioni di sicurezza e relativo registro: Data Breach procedure;
– Procedura per la gestione dei diritti degli interessati del trattamento: Procedura per l'esercizio dei diritti sui dati personali da parte dell'interessato (DSAR) (Data subject access requests);

• IT Security Policy – Dal punto di vista della sicurezza informatica, SCM Group ha definito regole e adottato un programma pervasivo e robusto per l'utilizzo degli strumenti informatici con l'obiettivo di mantenere l'integrità, riservatezza e disponibilità dei dati aziendali e personali e di proteggerli dalle minacce informatiche.

• Formazione per i dipendenti – Tutti i dipendenti di SCM Group ricevono informazioni sulle novità normative in materia di protezione dei dati personali e sono tenuti al completamento di corsi di

formazione finalizzati ad accrescere il livello di consapevolezza sui rischi e sulla normativa vigente in tema di protezione dei dati personali.

Data Protection Officer

SCM Group s.p.a ha nominato un Data Protection Officer, il quale svolge un ruolo di controllo anche nei confronti dei Privacy manager delle singole legal entity che compongono il Gruppo e con cui si interfaccia per garantire il corretto monitoraggio dei flussi di dati. Il Data Protection Officer riveste un ruolo di vigilanza sull'effettivo funzionamento delle misure tecniche e organizzative adottate, svolge anche un ruolo informativo e consultivo per tutti i soggetti aziendali preposti al trattamento e al governo dei dati e, infine, costituiscono il punto di riferimento per l'Autorità Garante e per gli interessati del trattamento. Il Data Protection Officer informa periodicamente gli organi amministrativi sul livello di esposizione al rischio data protection.

Nel corso del periodo di rendicontazione, il Data Protection Officer di SCM Group ha realizzato un'attività di monitoraggio compendiata in una relazione annuale, che è volta a valutare l'adeguatezza, lo stato di implementazione e l'efficacia operativa dei presidi e delle misure. I risultati di tale verifica sono stati portati all'attenzione degli organi di controllo e di governo aziendale, favorendo il consolidamento del piano di miglioramento continuo del sistema di data protection. Al fine di garantire una maggiore effettività dell'azione del Data Protection Officer del Gruppo, nel periodo di rendicontazione è stato definito una *data protection control framework*, che include le attività di controllo chiave soggette a periodico monitoraggio in modo da attivare flussi informativi che possano catturare tutte le dimensioni di rischio, per tutti i trattamenti presenti nel registro dei trattamenti dei dati personali.