FORNARI E ASSOCIATI
STUDIO LEGALE

FOCUS

Il Modello Organizzativo Privacy, gli altri modelli organizzativi e le possibili connessioni.

fornarieassociati.com

Milano • Roma • Bari

Aprile 2023

I. PREMESSA.

La protezione delle persone fisiche con riguardo al trattamento[1] dei dati di carattere personale è un diritto fondamentale sancito dall'art. 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione Europea e dall'art. 16, paragrafo 1, del Trattato sul Funzionamento dell'Unione Europea, che stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.

Come previsto dal Regolamento (UE) n. 2016/679 (di seguito, il "**GDPR**" o il "**Regolamento**") – in vigore dal 24 maggio 2016 – i principi e le norme a tutela delle persone fisiche con riferimento al trattamento dei dati personali[2] dovrebbero rispettarne i diritti e le libertà fondamentali, a prescindere dalla loro nazionalità e residenza.

Attraverso il GPDR, divenuto pienamente applicabile a partire dal 25 maggio 2018, la Commissione Europea si propone come obiettivo quello di assicurare un livello coerente ed elevato di protezione dei dati personali di tutte le persone fisiche presenti sul territorio dell'Unione Europea, attribuendo ai cittadini il controllo dei propri dati personali, semplificando il contesto normativo, unificando e rendendo omogeneo il livello di protezione dei diritti e delle libertà delle persone fisiche con riguardo al trattamento dei dati personali in tutti gli Stati Membri.

Al fine di armonizzare le norme previste dal legislatore italiano all'interno del D. Lgs. n. 196/2003 (di seguito, "**Codice Privacy**"), il 4 settembre 2018 è stato pubblicato in Gazzetta Ufficiale il D. Lgs. n. 101/2018 recante l'adeguamento della normativa nazionale al GDPR.

Tra i principi generali applicabili al trattamento dei dati, all'art. 5, paragrafo 2, il GDPR pone l'accento sul cd. principio dell'*accountability* del Titolare del Trattamento[3] (di seguito anche il "**Titolare**"),

[1] Ai sensi dell'art. 4, comma 1, numero 2) del GDPR il trattamento è: "*qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come 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*".

[2] Ai sensi dell'art. 4, comma 1, numero 1) del GDPR il dato personale è: "*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*".

[3] Ai sensi dell'art. 4, comma 1, numero 7) del GDPR il Titolare del Trattamento è: "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono*

vale a dire il principio di *"responsabilizzazione"* del Titolare, il quale non deve limitarsi ad osservare i criteri previsti dall'art. 5[4], ma deve essere in grado di adottare comportamenti proattivi, tali da dimostrare la concreta implementazione di misure finalizzate ad assicurare l'applicazione del predetto Regolamento (cfr. art. 24 GDPR).

A tal proposito, tra le misure ritenute più idonee ed efficaci in tema di *accountability*, si ritiene rientri l'adozione del Modello Organizzativo Privacy (di seguito, "MOP"). Trattasi del documento avente quale primaria finalità quella di dare evidenza delle azioni poste in atto da una organizzazione per far fronte agli adempimenti in materia di protezione dei dati.

II. Il MOP è una valida misura di *accountability* rispetto a quanto previsto dal GDPR?

Come già illustrato, nel percorso di adeguamento al GDPR è necessario individuare e adottare gli strumenti e le misure più adeguati ad assicurare che il trattamento dei dati personali avvenga conformemente alle condizioni prescritte dall'art. 5 del Regolamento.

Nel contempo, il GDPR impone al Titolare del Trattamento anche l'obbligo di dimostrare – su richiesta – che siano state adottate misure appropriate ed efficaci. Infatti, alla disposizione di cui all'art. 5 del GDPR fa da eco il considerando 74 che, coerentemente con il sopracitato art. 24 GDPR, prevede che "*il titolare del trattamento dovrebbe essere tenuto a mettere in atto misure adeguate ed efficaci ed essere in grado di dimostrare la conformità delle attività di trattamento con il presente regolamento, compresa l'efficacia delle misure* […]", e che tale capacità di comprovare il rispetto dei requisiti stabiliti dal GDPR deve persistere in ogni fase del percorso di adeguamento.

Richiamando espressamente l'*accountability*, principio cardine del GDPR, il Legislatore europeo chiede al Titolare del Trattamento di prevedere, predisporre e adottare misure tecniche e organizzative ritenute adeguate a gestire le attività di trattamento in modo da tutelare i diritti e le libertà degli interessati, in conformità con la normativa e principi del GDPR e, soprattutto, di essere in grado di dimostrare concretamente in ogni momento l'efficacia di tali misure.

Ciò posto, pur non essendo espressamente richiesto dal GDPR, si ritiene che il MOP, avendo l'obiettivo di riunire in un unico documento tutte le attività poste in essere in adeguamento alla normativa privacy, le motivazioni alla base delle scelte relative al trattamento dei dati nonché lo scadenziario degli adempimenti, possa rappresentare un'efficace misura di *accountability* per le organizzazioni aziendali. Ovviamente, è di fondamentale importanza che tale documento sia costantemente aggiornato, in occasione di variazioni di contesto impattanti sulla materia.

---

essere stabiliti dal diritto dell'Unione o degli Stati membri".

[4] Oltre al pilastro della "responsabilizzazione", i principi applicabili ai sensi dell'art. 5 del GDPR sono (*i*) liceità, correttezza e trasparenza; (*ii*) limitazione della finalità; (*iii*) minimizzazione dei dati; (*iv*) esattezza; (*v*) limitazione della conservazione; (*vi*) integrità e riservatezza.

III. In concreto, qual è la finalità di adottare un MOP?

Il MOP rappresenta uno specifico strumento pratico che consente al Titolare, a seconda della sua organizzazione, la scelta e la gestione responsabile e autonoma degli adempimenti in materia di protezione dei dati personali.

Nel contempo, tale atto consente di documentare e dimostrare in ogni momento:

- il rispetto dei principi fondamentali stabiliti dal GDPR;
- la conformità dei trattamenti effettuati al GDPR;
- l'efficacia delle migliori misure scelte e adottate nelle attività di trattamento;
- la continuità nel tempo del percorso di adeguamento intrapreso, anche a fronte di eventuali variazioni dell'assetto organizzativo aziendale;
- di aver intrapreso un percorso di *compliance* ben strutturato e definito, in grado di fornire anche alle autorità di controllo le necessarie coordinate nell'effettuazione dei controlli e delle verifiche.

Ovviamente, non esiste un modello unico ed esaustivo adatto ad ogni ente, bensì il documento dovrà essere calibrato in base alle peculiarità delle singole organizzazioni aziendali (sia al contesto interno, vedasi la tipologia di dati trattati, sia al contesto esterno, come le misure imposte dai soggetti esterni quali i Titolari del Trattamento), attraverso un metodo *tailor made*.

Per strutturare correttamente un MOP occorre fare riferimento al considerando 74 e all'art. 24 del GDPR, che forniscono delle linee guida per l'adozione di adeguate ed efficaci misure tecniche e organizzative.

In particolare, occorrerà tenere conto:

- della natura del trattamento;
- dell'ambito di applicazione;
- del contesto del trattamento;
- delle finalità del trattamento;
- dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche;
- dello stato dell'arte e dei costi di attuazione delle misure adeguate alla tutela dei dati personali, nonché della portata del trattamento (come indicato dall'art. 25 GDPR).

In particolare, l'art. 25 GDPR introduce dei principi essenziali sulla cui scorta delineare correttamente un MOP: si tratta dei principi di *privacy by design* e *privacy by default*, ovvero della "*protezione dei dati fin dalla progettazione*" e della "*protezione dei dati per impostazione predefinita*".

In funzione dell'approccio del GDPR, incentrato sulla valutazione del rischio, i predetti principi impongono al Titolare del Trattamento o al Responsabile del Trattamento[5] (di seguito anche il "**Responsabile**") – sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso – di mettere in atto misure tecniche e organizzative adeguate, volte ad attuare in modo efficace i principi di protezione dei dati, e a integrare nel trattamento le necessarie garanzie al fine

[5] Ai sensi dell'art. 4, comma 1, numero 8) del GDPR il Responsabile del Trattamento è: *"la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento"*.

di soddisfare i requisiti del GDPR e di tutelare i diritti degli interessati.

In sostanza, la finalità primaria del MOP è quella di condensare in un unico testo, a beneficio di tutte le parti interessate, una serie di documenti che altrimenti potrebbe essere difficile inventariare e monitorare, soprattutto per realtà aziendali di medio-grandi dimensioni, nelle quali la documentazione afferente alla protezione dei dati tende a proliferare.

IV. COM'È STRUTTURATO IL MOP?

Si è detto che attraverso il MOP l'organizzazione interessata può ordinare sistematicamente tutte le procedure e le misure adottate e quelle da implementare nel percorso di adeguamento alla privacy, con la relativa documentazione.

Nella prassi, il MOP potrà essere strutturato al fine di dare conto e raccogliere in ordine sistematico:

- le disposizioni normative che regolano il settore di appartenenza dell'organizzazione in ambito privacy. Infatti, il MOP contiene o fa riferimento a procedure, istruzioni, modelli ed altri documenti che l'organizzazione potrebbe aver predisposto per dare evidenza dell'applicazione della normativa. Ciò in ossequio ad uno dei principi fondamentali della documentazione sui sistemi di gestione, il quale richiede che non si duplichino testi aventi i medesimi contenuti in documenti differenti. Le parti componenti il MOP, a loro volta, possono essere utilizzate quali criteri di audit;
- la definizione dei principi e dei termini fondamentali in ambito privacy in relazione alla natura dei trattamenti effettuati;
- la descrizione dell'organizzazione e la tipologia dei trattamenti di dati personali. Come anticipato, il MOP deve essere aggiornato in occasione di variazioni di contesto (interno o esterno all'organizzazione), di aggiornamenti normativi, in caso di introduzione di nuove misure oppure in seguito alla modifica o eliminazione di misure ritenute non più adeguate. È opportuno conservare lo storico delle diverse versioni del documento per comprenderne, nel tempo, l'evoluzione;
- la mappatura dei flussi informativi e la tipologia di dati trattati;
- l'organigramma del Titolare del Trattamento;
- le informative (ad esempio, informative privacy per clienti, personale, fornitori, utenti esterni o modelli di consenso al trattamento);
- i ruoli, le funzioni e le responsabilità del Titolare, nonché dei soggetti delegati al trattamento dei dati personali;
- i rapporti contrattuali tra Titolare, contitolari, Responsabili del Trattamento e, se nominato, del Responsabile della Protezione dati (di seguito "DPO"[6]) e le relative responsabilità;

[6] Ai sensi dell'art. 37, comma 1 del GDPR: *"Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta: a) il trattamento è*

- gli atti di nomina degli autorizzati interni al trattamento, con le relative competenze, doveri, ruoli e responsabilità (*ex* artt. 2-*quaterdecies* del Codice Privacy e 29 del GDPR);
- le attività di formazione del personale, predisponendo un sistema che documenti la formazione svolta per ciascun soggetto (art. 39 del GDPR);
- le procedure di comportamento del personale interno e le policy di utilizzo dei sistemi e dispositivi elettronici, *e-mail*, internet, e dei sistemi di archiviazione elettronica;
- le procedure di audit per verificare la *compliance* al GDPR;
- la valutazione delle misure tecniche e organizzative per garantire livelli di sicurezza adeguati al rischio (art. 32, par. 2, GDPR);
- la documentazione inerente al riesame, agli aggiornamenti e all'implementazione delle misure tecniche e organizzative adottate;
- la procedura di valutazione dei rischi ("**Risk Assessment**") *ex* art. 32, paragrafo 2, GDPR, e la procedura di valutazione di impatto (cd. "**DPIA**") dei trattamenti previsti sulla protezione dei dati in presenza di rischi elevati per i diritti e le libertà degli interessati;
- le prassi operative in caso di violazioni di dati (cd. "**Data Breach**")[7] e di incidenti della sicurezza sia per la propria organizzazione che per gli eventuali responsabili del trattamento e/o contitolari;
- le procedure per l'esercizio dei diritti degli interessati;
- i modelli di notifica al Garante *ex* art. 33 in caso di Data Breach e di comunicazione agli interessati *ex* art. 34 GDPR, nonché il modello di richiesta di esercizio dei diritti degli interessati e di riscontro da parte dell'organizzazione;
- l'adozione di codici di condotta e/o modelli organizzativi *ex* D. Lgs. n. 231/2001;
- le certificazioni aziendali.

Nel caso di un gruppo di imprese, il MOP si occupa altresì di chiarire e definire (*i*) il ruolo e le responsabilità delle singole società all'interno del gruppo; (*ii*) i rapporti interni e con la *holding*; (*iii*) le modalità di trasferimento dei dati tra le singole entità; (*iv*) le finalità dei trattamenti effettuati da ciascuna entità.

effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali; b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10".

[7] Ai sensi dell'art. 33, comma 1 del GDPR: *"In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo".*

V. Quali sono i destinatari del MOP?

I destinatari del MOP sono:

- il DPO (quando presente);
- il Titolare del Trattamento, nel caso in cui l'organizzazione – che ha predisposto il MOP – rivesta il ruolo di Responsabile (in tal caso, a quest'ultimo soggetto dovrebbe essere consentito solo un accesso parziale al MOP);
- gli incaricati dell'attività di audit/ispezione;
- gli autorizzati al trattamento (anche in questo caso è possibile sia consentito solo un accesso parziale al documento);
- altri eventuali soggetti in rappresentanza delle parti interessate.

L'accesso al documento deve, in ogni caso, essere autorizzato dalla direzione dell'organizzazione.

In merito ai soggetti coinvolti, il MOP viene di norma redatto dal Referente Privacy o dal *Privacy Officer* ed approvato dal Titolare del Trattamento. Quando è designato un DPO, quest'ultimo esprime una valutazione sul documento, richiedendo, ove ritenute necessarie, le opportune modifiche ed integrazioni.

VI. Sono previsti degli standard da rispettare ai fini della redazione del MOP?

Nella redazione del MOP è utile tenere in considerazione anche gli standard previsti dalle normative ISO, in particolare la ISO/IEC 27701, per la gestione delle informazioni personali e della privacy (che ha aggiornato le normative precedenti quali la ISO/ IEC 27001:2017 e la ISO/IEC 27002), volta a fornire uno strumento pratico alle organizzazioni per (*i*) implementare il sistema di gestione e sicurezza dei dati personali; (*ii*) documentare le scelte di natura tecnica e organizzativa adottate; (*iii*) migliorare i controlli e le verifiche interne e (*iv*) coordinarsi con le autorità di controllo per le verifiche del caso.

In alternativa alla poc'anzi citata norma, l'altra possibile (e valida) opzione è quella di guardare alle *best practices* indicate dalla ISO 29100, pubblicata nel 2011 e aggiornata nel 2015, finalizzata a definire un manuale operativo in ambito privacy.

In ogni caso, a prescindere dall'integrazione o meno degli standard sopra descritti, è fondamentale che il MOP racchiuda tutte le attività di adeguamento privacy poste in essere e da implementare, nonché che il documento sia aggiornato con frequenza.

VII. Quali sono i vantaggi nell'adottare il MOP?

Affinché il MOP possa rivelare la propria utilità anche sul piano organizzativo, lo stesso dovrà essere portato a conoscenza di tutti i soggetti – che operano all'interno dell'organizzazione – coinvolti nelle attività di trattamento dei dati personali, unitamente alla documentazione elaborata in ambito privacy.

In particolare, tali documenti devono essere fruibili e visionabili da tutti i dipendenti e collaboratori per migliorare il coordinamento e il dialogo tra le diverse funzioni aziendali, permettendo di mantenere un costante

percorso di adeguamento anche nel caso di modifiche dell'organizzazione aziendale.

L'adozione di un MOP, come già accennato, permette inoltre all'organizzazione di rispettare il dovere di collaborazione con le autorità di controllo nelle ispezioni e nell'esecuzione dei loro compiti, come stabilito espressamente dagli artt. 30, paragrafo 4, e 31 del GDPR.

Il MOP rappresenta quindi per le organizzazioni che trattano dati personali, insieme al registro delle attività di trattamento[8] e al registro dei Data Breach, uno strumento fondamentale per l'attuazione del GDPR.

Infine, la maggiore utilità che può derivare ad una organizzazione discende dalla capacità di far dialogare tra loro tutti i modelli organizzativi adottati. In questo senso, il MOP può rappresentare il punto di riferimento e di raccordo per tutti i modelli organizzativi precedentemente adottati, rappresentando il trattamento dei dati personali un'attività trasversale ad ogni settore aziendale.

VIII. Quali sono i punti di contatto tra il MOP e il Modello 231?

Parlare di MOP richiama immediatamente alla mente il Modello di Organizzazione di cui al D. Lgs. n. 231/2001 (di seguito "**Modello 231**").

Come noto, il D. Lgs. n. 231/2001 disciplina la responsabilità degli enti per gli illeciti amministrativi dipendenti da reato e consente di eliminare o attenuare il rischio e le conseguenze delle gravose sanzioni connesse alla commissione di particolari reati (cd. "**Reati Presupposto**"), similmente all'art. 30 del D. Lgs. n. 81/2008 ("Testo unico in materia di tutela della salute e della sicurezza nei luoghi di lavoro"). Infatti, anche il predetto Testo Unico prevede la possibilità di istituire un idoneo modello di organizzazione e di gestione con efficacia esimente della responsabilità amministrativa dell'ente nel caso di reati in materia di salute e sicurezza sul lavoro.

L'adozione del Modello 231 è dunque un elemento difensivo di grande importanza per la difesa delle organizzazioni aziendali nell'ambito di processi penali in cui l'ente risulti imputato, purché il Modello 231 in concreto adottato risulti idoneo "*a prevenire reati della specie di quello verificatosi*"[9].

Diversamente da quanto previsto dal D. Lgs. n. 231/2001, il GDPR non è costruito attorno a uno specifico modello organizzativo e non prevede, quindi, un contenuto minimo inderogabile.

Ciò nonostante, alcuni degli adempimenti previsti dal GDPR trovano una loro corrispondenza o similitudine con quelli che rappresentano il contenuto minimo del Modello 231 *ex* artt. 6 e 7 del D. Lgs. n. 231/2001:

- individuare le attività di trattamento di dati personali più esposte al rischio di violazioni e procedere a una valutazione di impatto sul trattamento quando questo presenta rischi elevati

[8] Ai sensi dell'art. 30, comma 1 del GDPR: *"Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità*".

[9] Art. 6 del D. Lgs. n. 231/2001.

per i diritti e le libertà delle persone fisiche coinvolte (art. 35 GDPR – *cfr.* art. 6, comma 2, lett. A, D. Lgs. n. 231/2001);

- prevedere e programmare misure di formazione per assicurare che coloro i quali agiscono sotto il Titolare (o il Responsabile) siano adeguatamente istruiti affinché il trattamento sia effettuato conformemente al GDPR e garantisca la tutela dei diritti degli interessati (art. 29 GDPR – *cfr.* art. 6, comma 2, lett. B e D, D. Lgs. n. 231/2001);

- mettere in atto misure tecniche e organizzative adeguate sia per realizzare efficacemente i principi di protezione dei dati "*by design" e "by default*", tenendo conto anche dei costi di attuazione, sia per garantire un livello di sicurezza adeguato al rischio (artt. 25 e 32 GDPR – *cfr.* art. 6, comma 2, lett. C, D. Lgs. n. 231/2001);

- ove si ravvisasse una violazione di dati personali degli interessati, adottare misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati anche successivamente al verificarsi di un Data Breach, rivedendo e implementando le misure adottate (art. 34 GDPR – *cfr.* art. 7, comma 4, D. Lgs. n. 231/2001);

- procedere al riesame della valutazione d'impatto sulla protezione dei dati quando insorgono variazioni del rischio nelle attività di trattamento (art. 35 GDPR – *cfr.* art. 7, comma 4, D. Lgs. n. 231/2001);

- procedere al riesame e all'aggiornamento delle adottate misure tecniche e organizzative quando necessario, nonché ad un'integrazione delle garanzie necessarie per soddisfare i requisiti del GDPR anche nel corso del trattamento (art. 35 GDPR – *cfr.* art. 7, comma 4, D. Lgs. n. 231/2001).

In aggiunta, entrambi i modelli sono costruiti su un approccio fondato sulla valutazione del rischio, ponendo al centro il principio di responsabilizzazione dell'organizzazione, e prevedono la possibilità di riferirsi a codici di condotta per dimostrare la conformità alle normative di riferimento (art. 32 GDPR e art. 6 D. Lgs. n. 231/2001).

Non solo, naturalmente entrambi i documenti devono essere costruiti sulla base delle caratteristiche peculiari di ciascuna realtà aziendale, in un percorso di costante adeguamento che tenga conto anche dell'evoluzione dell'organizzazione.

Infine, entrambi i modelli – ancorché per finalità differenti – sono volti a prevenire il rischio di un trattamento illecito dei dati personali. Da una parte, il sistema di controllo previsto dal D. Lgs n. 231/2001 è finalizzato alla prevenzione dei reati nell'interesse o a vantaggio dell'organizzazione, includendo tra i Reati Presupposto anche i delitti informatici e l'illecito trattamento dei dati (art. 24-*bis* D. Lgs. n. 231/2001); dall'altra parte, il GDPR ha quale obiettivo la tutela dei diritti e delle libertà fondamentali degli interessati.

Tuttavia, i modelli differiscono principalmente per il fatto che con l'adozione preventiva di un efficace Modello 231, l'ente può, oltre che prevenire, escludere la propria responsabilità per reati commessi dai membri della propria organizzazione.

Viceversa, l'adozione di un MOP non consente di per sé di escludere la responsabilità dell'organizzazione in caso di Data Breach e/o di inadempimento dei principi e delle norme del GDPR.

IX. Ci sono connessioni tra il MOP e gli altri modelli e sistemi di gestione?

L'integrazione tra norme e sistemi è un tema di grande attualità, a cui sono dedicati standard specifici come la recente ISO 37301:2021 "*Sistemi di gestione per la compliance - Requisiti con guida per l'utilizzo*" che fornisce le "*Linee guida per istituire, sviluppare, attuare, valutare, mantenere e migliorare un efficace sistema di gestione per la compliance all'interno di un'organizzazione*".

Il MOP per sua natura tende a favorire l'integrazione, a beneficio di tutte le parti interessate, per gestire nel modo più efficiente i dati personali, nel rispetto della normativa e delle procedure interne.

Infatti, il documento contiene o richiama procedure predisposte per documentare i processi aziendali, tenendo in considerazione anche le implicazioni in materia di privacy.

Di seguito si riportano alcuni esempi di integrazione di sistemi di gestione:

- la procedura sulla gestione dei rifiuti elettronici impatta sui temi dell'ambiente, della sicurezza delle informazioni e della protezione dei dati personali (in proposito, le norme di riferimento sono rappresentate dal D. Lgs. n. 49/2014, dalla UNI EN ISO 14001:2015; dalla ISO/IEC 27001:2022 e dal GDPR);

- la procedura sulla gestione degli infortuni concerne tematiche che riguardano la salute e sicurezza dei lavoratori e la protezione dei dati personali (in proposito, le norme di riferimento sono date dal D. Lgs. N. 81/2008, dalla UNI ISO 45001:2018 e dal GDPR);

- la procedura per la valutazione dei fornitori tiene in considerazione (i) la capacità di fornire un servizio/prodotto in linea con le esigenze aziendali; (ii) il monitoraggio delle prestazioni; (iii) le garanzie fornite nel ruolo di Responsabili del Trattamento (a tal proposito, le norme di riferimento sono la UNI EN ISO 9001:2015, la ISO/IEC 27001:2022, la ISO/IEC 27701:2019 e il GDPR).

X. Quali sono i benefici di un sistema di gestione integrato?

L'obiettivo dell'integrazione consiste nel condensare in un numero limitato di documenti tutti gli aspetti afferenti ai processi aziendali per garantirne una gestione organica evitando la duplicazione di regole che potrebbero in parte sovrapporsi o rischiare di essere in contraddizione. In altre parole, dunque, il sistema di gestione integrato consente di evitare duplicazioni di

procedure tra più sistemi e di prevenire o eliminare possibili conflitti tra normative.

In aggiunta all'unicità documentale, l'adozione di un sistema integrato consente di:

- creare sinergie tra processi aziendali che interessano trasversalmente l'organizzazione aziendale;
- unificare gli obiettivi aziendali;
- semplificare i rapporti tra le funzioni aziendali;
- valutare e quindi prevenire i rischi aziendali secondo un approccio unitario.

CONTATTI

Giuseppe Fornari
Founder Partner

g.fornari@fornarieassociati.com

Pasquale Grella
Of Counsel

p.grella@fornarieassociati.com

Caterina Peroni
Associate

c.peroni@fornarieassociati.com

Milano
Via Chiossetto 18
T: +39 0254122206
E: milano@fornarieassociati.com

Roma
Piazza di San Lorenzo in Lucina 26
T: +39 0622201000
E: roma@fornarieassociati.com

Bari
Via Principe Amedeo 25
T: +39 0809184280
E: bari@fornarieassociati.com