Newsletter
Maggio 2019

LA COGENZA DEL REGOLAMENTO EUROPEO 679/2016 (GDPR) NEL SISTEMA DI GESTIONE PER LA QUALITA'

Care Colleghe, Cari Colleghi,

Vi trasmettiamo la Newsletter di Maggio 2019 dal titolo *La cogenza del Regolamento Europeo 679/2016 (GDPR) nel Sistema di Gestione per la Qualità*, che segue le precedenti newsletter relative agli Schemi di Certificazione di AICQ SICEV.

Questa "pillola" formativa ci è stata messa a disposizione dal collega ed amico Attilio Rampazzo - nostro Referente per diversi Schemi di Certificazione - tra cui quello relativo al "Trattamento e protezione dei dati personali", e tratta un argomento di estremo interesse per tutti gli Auditor/Lead Auditor iscritti nei nostri Registri:

la valutazione dei "requisiti cogenti di prodotto/servizio" nell'ambito della valutazione dei Sistemi di Gestione in generale e di quelli per la Qualità in particolare.

La cogenza di prodotto/servizio considerata questa volta è quella riferita al Regolamento Europeo 679/2016 (GDPR). Siccome la materia trattata è molto critica abbiamo preferito integrare la Newsletter preparata da Attilio Rampazzo con il parere autorevole del Servizio Legale di ACCREDIA.

Vi raccomandiamo pertanto di leggere con molta attenzione la seguente Newsletter e di intraprendere le azioni conseguenti secondo la Vostra necessità individuali.

Buona lettura!

Roberto Pietri
Direttore AICQ SICEV

Know how in pillole

Con l'espressione Sistema di Gestione si può fare riferimento a tutti gli schemi normativi che, ciascuno con un diverso oggetto (es. qualità, sicurezza delle informazioni, *business continuity*, ambiente, sicurezza sul lavoro, privacy, prevenzione degli illeciti ...), prescrivono ad un'Organizzazione la definizione di manuali, procedure scritte, regolamenti interni, registrazioni,

sessioni di formazione ed addestramento del personale, audit e controlli interni, tracciabilità di tutte le operazioni poste in essere ed ogni altro adempimento idoneo ad attestare il rispetto di una norma giuridica o tecnica. I Sistemi di Gestione sono ormai una realtà diffusa nel diritto d'impresa, a livello nazionale e comunitario, e determinano, in molti casi, la crescita esponenziale degli adempimenti e dei conseguenti costi, senza che a ciò corrisponda, il più delle volte, un effettivo beneficio.

D'altra parte sia la norma ISO 9001 che il Regolamento UE 679/16 attuano un approccio *Risk Based Thinking* che presume, documentando le scelte intraprese, di identificare i fattori di rischio, verificandone i livelli di esposizione e di gestirli attraverso misure e controlli idonei a minimizzarne gli effetti negativi e massimizzarne le opportunità, innalzando il livello di tutela dell'Organizzazione.

Ne emerge che tra normazione e legislazione esiste un rapporto stretto ma anche complesso. Se infatti l'applicazione delle norme è volontaria, quando queste vengono richiamate nei provvedimenti legislativi può intervenire un livello di cogenza, delimitato pur sempre dal contesto di riferimento. Sono infatti numerosi i provvedimenti di legge che fanno riferimento, genericamente o con preciso dettaglio, alle norme, a volte obbligatoriamente, altre solo come via preferenziale (ma non unica), verso il rispetto della legge.

La norma UNI EN ISO 9001 specifica i requisiti di un Sistema di Gestione per la Qualità quando un'Organizzazione:

- *ha l'esigenza di dimostrare la propria capacità di **fornire** con regolarità **prodotti o servizi che soddisfano** i requisiti del cliente e **i requisiti cogenti applicabili***
- *mira ad accrescere la soddisfazione del cliente tramite l'applicazione efficace del Sistema, compresi i processi per migliorare il Sistema stesso ed **assicurare la conformità** ai requisiti del cliente e ai **requisiti cogenti applicabili***

e ribadisce che *fra i benefici potenziali per un'Organizzazione, derivanti dall'attuazione di un Sistema di Gestione per la Qualità basato sulla presente norma internazionale, c'è la capacità di fornire con regolarità prodotti e servizi che soddisfino i **requisiti** del cliente e quelli **cogenti applicabili*** (si tratta delle cogenze di prodotto/servizio, quali ad esempio le direttive sulla Marcatura CE, e non quelle di tipo generale).Tra l'altro, il termine cogente viene trovato nella norma ben 14 volte ed, in particolare, nel capitolo 8 "Attività Operative" il termine è presente 5 volte.

Nel caso del Regolamento UE 679/2106, si tratta di una cogenza importante che ogni Organizzazione deve adempiere per rispettare le leggi dello Stato Italiano. Diverso invece è il criterio con cui tale Regolamento possa o meno essere considerato come una delle cogenze di prodotto/servizio ai fini di una certificazione ISO 9001.

Nel rispetto del documento IAF ID 1 revisione 2 del 10/06/2014, la norma UNI EN ISO 9001 può essere applicata ad una vasta gamma di Organizzazioni la cui attività viene identificata tramite apposite tabelle settoriali. Anche i citati requisiti cogenti di prodotto/servizio devono essere interpretati in base al settore nel quale opera l'Organizzazione. Infatti il GDPR, o Regolamento EU 679/16, avrà implicazioni diverse in un'Organizzazione che produce oggetti metalmeccanici rispetto ad un'Organizzazione informatica o di servizi commerciali o di servizi sanitari, nella quale i dati personali o il loro trattamento tendenzialmente sono un "must" per offrire attività alla clientela. Per chiarire ulteriormente quanto detto si ricorda che, ad esempio, in occasione di un audit di 3° parte di un'Organizzazione del settore IAF 18 (Macchine, apparecchi, impianti meccanici) un Auditor deve verificare la corretta applicazione della Direttiva Macchine essendo una cogenza di prodotto. Invece, in una Organizzazione del settore IAF 13 (Prodotti Farmaceutici) la citata Direttiva Macchine non può essere considerata una cogenza di prodotto.
E' però necessario individuare un criterio equilibrato e ragionevole per mantenere in equilibrio i due piatti della bilancia: il carattere volontario del Sistema di Gestione di una Organizzazione e la rilevanza dei requisiti cogenti di prodotto/servizio secondo la ISO 9001 e definire il livello d'indagine che spetta ad un Auditor di un Organismo di Certificazione in merito al rispetto dei citati requisiti cogenti.

Si deve ovviamente escludere che un audit di certificazione possa occuparsi di tutte le leggi che in qualche misura sono collegate ai singoli requisiti della Norma, giacché, in tal caso, l'audit sarebbe impossibile allo stato attuale del funzionamento del sistema di certificazione e di accreditamento. Né si può sostenere che un certo settore normativo, ad esempio la protezione dei dati personali, sia "gerarchicamente" più significativa di altri. Ai requisiti della Norma ISO 9001, infatti, si potrebbero facilmente ricollegare, ad esempio, tutte le norme in materia di sicurezza e salute sul lavoro o di diritto del lavoro.

Diverso è il caso dei requisiti cogenti, di prodotto/servizio, che sono legati in modo diretto allo specifico campo di applicazione del Sistema di Gestione di una Organizzazione e che non possono

non essere tenuti in considerazione in occasione di un audit di certificazione (ad esempio, la verifica delle necessarie autorizzazioni amministrative per una struttura sanitaria).

In conclusione, è ragionevole affermare che un Organismo di Certificazione debba verificare che una Organizzazione abbia considerato, nel definire il proprio Sistema di Gestione, i requisiti di rango legislativo che in modo diretto abbiano impatto sulla qualità del prodotto fornito o del servizio erogato.

E' ragionevole escludere che possa competere ad un auditor di un Organismo di Certificazione una verifica puntuale in ordine al rispetto da parte di una Organizzazione di singole norme cogenti, il che trasformerebbe l'audit di certificazione in un audit di legalità. L'analisi da parte dell'Auditor deve limitarsi alla verifica in merito alla capacità di una Organizzazione di tenere sotto controllo il rispetto dei requisiti cogenti, nei termini generali che appartengono ad un Sistema di Gestione per la Qualità.

Ad esempio, un'Organizzazione dovrà:

- avere individuato i requisiti cogenti relativi al proprio Sistema di Gestione ed ai prodotti/servizi correlati;
- gestire come non conformità le violazioni a requisiti cogenti;
- dedicare una sezione del riesame della direzione alla verifica del rispetto dei requisiti cogenti;
- promuovere la formazione e l'aggiornamento del personale in merito alle norme più rilevanti per la propria attività;
- individuare tra i fornitori esterni le risorse professionali necessarie per garantire le conoscenze anche in ambito legale;
- inserire nei programmi di audit di prima parte verifiche in ordine al rispetto dei più importanti requisiti cogenti.

Si tratta, in questi casi, di necessarie verifiche dirette a garantire un'Organizzazione improntata anche a soddisfare i requisiti cogenti.

Diverso sarebbe imporre agli auditor di un Organismo di Certificazione la verifica del rispetto di singole misure normative, il che porrebbe l'audit al di fuori dell'attuale meccanismo di certificazione volontaria.

Rispetto alla questione del rapporto tra GDPR e certificazione ISO 9001, l'utilizzo di tali criteri determina quindi la seguente conclusione:

- per le Organizzazioni che trattano dati personali in modo significativo (come nel caso prospettato della struttura sanitaria) è certamente necessario verificare che una Organizzazione abbia considerato il GDPR tra i requisiti applicabili e si sia dotata di strumenti organizzativi, quali quelli sopra indicati e compresa la nomina del DPO ove obbligatoria in base al Regolamento ed alle indicazioni del Garante, diretti ad assicurare la protezione dei dati personali in modo adeguato;
- non compete invece agli Auditor dell'Organismo verificare il rispetto delle singole prescrizioni del GDPR, ciò che spetta invece all'autorità pubblica a ciò preposta dalle norme in vigore.

A titolo esemplificativo e non esaustivo, sono state individuate le seguenti categorie di soggetti (tratti dalle FAQ del Garante Privacy Italiano) che certamente sono tenute alla nomina di un DPO e per le quali in sede di un audit ISO 9001 di 3° parte deve sicuramente essere verificata l'applicazione del GDPR nei termini definiti in precedenza:

- istituti di credito;
- imprese assicurative;
- sistemi di informazione creditizia;
- società finanziarie;
- società di informazioni commerciali;
- società di revisione contabile;
- società di recupero crediti;
- istituti di vigilanza;
- partiti e movimenti politici; sindacati;
- caf e patronati;
- società operanti nel settore delle "utilities" (telecomunicazioni, distribuzione di energia elettrica o gas);
- imprese di somministrazione di lavoro e ricerca del personale;
- società operanti nel settore della cura della salute, della prevenzione/diagnostica sanitaria quali ospedali privati, terme, laboratori di analisi mediche e centri di riabilitazione;

- società di call center;
- società che forniscono servizi informatici;
- società che erogano servizi televisivi a pagamento.

Per le sopracitate categorie, la mancata o incompleta applicazione del GDPR determina l'emissione di una Non Conformità che, in base alla sua classificazione (minore o maggiore) può diventare ostativa per il rilascio della certificazione ISO 9001 di un'Organizzazione.

Vediamo quali sono i principali punti di contatto operativi e di contenuti tra la norma UNI EN ISO 9001 ed il Regolamento UE 679/16:

UNI EN ISO 9001:2015	REGOLAMENTO UE 679/2016
§ 4.1 Comprendere l'Organizzazione ed il suo contesto L'Organizzazione deve determinare i fattori esterni e interni e indirizzi strategici che influenzano la sua capacità di conseguire i risultati attesi per il proprio sistema di gestione per la qualità	Art. 24 Responsabilità del Titolare del trattamento Il Titolare del trattamento tenuto conto del contesto, delle finalità del trattamento e dei rischi per i diritti e le libertà delle persone fisiche, deve determinare strategie adeguate in materia di protezione dei dati conformi al regolamento
§ 8.5.3 Proprietà che appartengono ai clienti o fornitori esterni L'Organizzazione deve identificare, verificare, proteggere e salvaguardare la proprietà del cliente o del fornitore esterno Nota: La proprietà del cliente o del fornitore esterno comprende anche materiali, strumenti, siti o dati personali	Artt. 12 -13 – 14 Informazione per l'interessato Definizione delle modalità per l'esercizio dei diritti dell'interessato, le informazioni da fornire qualora i dati personali siano raccolti o no presso l'interessato
§ 8.7 Controllo degli output non conformi L'Organizzazione deve assicurare che gli output non conformi ai requisiti siano identificati e tenuti sotto controllo	Art. 33 Notifica di una violazione dei dati personali all'autorità di controllo In caso di violazione dei dati personali, il Titolare del trattamento, deve notificare la violazione all'Autorità di controllo
§ 9.1.2 Soddisfazione del cliente L'Organizzazione deve monitorare le percezioni del cliente riguardo al grado in cui le sue esigenze e aspettative sono state soddisfatte	Artt. 15-16-17-18-19 Diritti dell'interessato Art. 34 Comunicazione di una violazione dei dati personali all'Interessato

Ed ancora altre sinergie:

UNI EN ISO 9001:2015	Applicazione GDPR
"L'Organizzazione deve mettere a disposizione le persone necessarie per l'attuazione del SGQ (par. 7.1.2 della norma ISO 9001)"	Se rientra nei casi previsti dal Regolamento Europeo Privacy, o da quanto consigliato dal Garante Privacy va designato un Responsabile della Protezione dei Dati (DPO).
"L'Organizzazione deve mettere a disposizione l'infrastruttura necessaria per l'attuazione del SGQ (par. 7.1.3 della norma ISO 9001)"	Non bisogna dimenticarsi anche sistemi hardware e software, antivirus, antimalware, back up, piano di disaster recovery (ovvero strumenti che garantiscano anche la protezione dei dati personali gestiti in formato elettronico)
L'Organizzazione deve assicurare che le persone siano competenti ed eventualmente deve formarle (par. 7.2 della norma ISO 9001)".	Il che significa che, se occorre, si dovrà formare un DPO. Ma non solo, la formazione ha un ruolo fondamentale in generale per le risorse umane, capitale umano che deve essere valorizzato, e all'interno dello stesso GDPR è prevista formazione obbligatoria.
"L'Organizzazione deve assicurare che le persone siano consapevoli …. del proprio contributo all'efficacia del SGQ, compresi i benefici derivanti dal miglioramento delle prestazioni (par. 7.3 della norma ISO 9001)".	Il che significa che all'atto di una nuova assunzione, o di un cambio di mansione, si dovrà preparare la lettera di nomina incaricato/addetto al trattamento dei dati personali per rendere consapevole la persona stessa dell'importanza della corretta gestione del trattamento dei dati personali.
"L'Organizzazione deve assicurare che i processi, prodotti e servizi forniti dall'esterno non influenzino negativamente la capacità dell'organizzazione di rilasciare con regolarità ai propri clienti, prodotti e servizi conformi (par. 8.4.2 della ISO 9001)":	In base alla tipologia di servizio reso da un fornitore, potrebbe esserci la necessità di nominarlo responsabile esterno del trattamento dati oppure amministratore di sistema. (vedere anche recenti interpretazioni del Garante della Privacy relativamente al Responsabile esterno del Trattamento).
"L'Organizzazione deve aver cura della proprietà dei clienti (par. 8.5.3 della ISO 9001)":	Per proprietà dei clienti si intendono anche i dati personali. L'Organizzazione deve quindi dichiarare come utilizza i dati personali, come li conserva e li protegge, come li recupera, se sono conservati su supporti informatici.

Da ciò emerge una riflessione importante che impone agli auditor di SGQ ISO 9001, in sede di audit di 2ª e 3ª parte, in particolar modo, di includere nel loro Piano di Audit la verifica del livello di osservanza del GDPR in relazione al settore merceologico in cui opera l'Organizzazione oggetto dell'audit. Nelle imprese operanti nei settori dell'*Information Technologies* delle Telecomunicazioni, ad esempio, il Gruppo di Audit dovrà verificare il grado di applicazione ed osservanza della

legislazione vigente in materia di protezione dei dati personali con riferimento al Regolamento Ue 679/2016, essendo questo strettamente connesso alla fornitura di servizi. Pertanto, in sede di audit secondo la ISO 9001, al di là di qualunque pensiero e convincimento personale, c'è da chiedersi se la Non Conformità rispetto ad un requisito cogente sia da considerarsi tale da impedire, interrompere o revocare il processo di certificazione (nel caso di Organizzazioni appartenenti alle categorie sopracitate) o, diversamente, sia necessario solo emettere una raccomandazione di miglioramento (nel caso di Organizzazioni non incluse nelle citate categorie).Quanto sopra ci fa capire come l'integrazione all'interno di un SGQ già esistente della parte documentale relativa alla gestione dei dati personali possa essere un vantaggio non da poco.

Vediamo nel dettaglio quali sono i documenti (requisiti) da tenere sotto controllo per il rispetto del Regolamento UE 679/16:

- Registro dei Trattamenti (anche se richiesto per Organizzazioni con un minimo di 250 dipendenti ma essenziale per poter verificare i successivi adempimenti);
- informative (dovrebbe essercene una per ogni trattamento);
- consensi (rispetto al precedente D.lgs. 196 sono necessari solo per i trattamenti che si basano sul consenso);
- lettere di incarico degli addetti al trattamento con precise istruzioni;
- elenco degli addetti al trattamento;
- nomina dei responsabili esterni dei trattamenti;
- elenco dei responsabili esterni dei trattamenti;
- misure di sicurezza idonee (queste vanno individuate in base ad una analisi dei rischi: devono essere logiche, gestionali e fisiche …);
- un sistema di verifiche (audit interni) sul rispetto del Regolamento UE 679/16;
- modalità di privacy by design e by default.

La mancanza anche di uno dei punti in elenco, in caso di controllo/verifica del Garante della Privacy (o Nucleo Speciale Privacy della Guardia di Finanza), comporterebbe sicuramente sanzioni, talvolta consistenti, previste dal Regolamento UE 679/16. Pertanto, sarà compito dell'auditor che rileva eventuali mancanze definirne anche la classificazione (minore o maggiore).

La protezione dei dati personali è percepita talvolta come una seccatura, un costo inutile e per tale motivo si cercano strade alternative per risolvere o bypassare il problema, tuttavia, i punti in comune che hanno il Sistema di Gestione Qualità ed il Regolamento UE 679/2016 sono veramente basilari per ogni Organizzazione, anche quelle di ridotte dimensioni, ad esempio:

- approccio basato sull'analisi del rischio;
- applicabilità a tutte le imprese private o pubbliche a prescindere dal settore e dal business (anche se le modalità di applicazione variano per categoria di Organizzazione;
- impostazione volta ad evitare la perdita di dati personali preziosi per le Organizzazioni e per le loro parti interessate;
- verifiche periodiche sulla modalità di trattamento e protezione dei dati personali.

Ogni Organizzazione che gestisce dati personali e particolari attraverso computer, server, supporti informatici o cartacei può trarre senza dubbio numerosi vantaggi dall'integrazione di un SGQ con il Regolamento UE 679/2016. Per far questo è necessario offrire al mercato un sistema di misura e di valutazione delle professionalità credibile e qualificato.

A cura di

Attilio Rampazzo CISA, CRISC, C|CISO CMC
Information Systems Consultant, Trainer & Auditor European Data Protection Expert
Auditor RGVI QMS ISMS ITSMS BCMS (Registri AICQ SICEV) Data Protection Officer - Data Protection Auditor (Registri AICQ SICEV). Referente Registri AICQ SICEV professionisti ICT e Protezione Dati Personali

e-mail: attilio@rampazzo.it

www.aicqsicev.it
info@aicqsicev.it
+39 0266713425