SEMINARIO ISTITUZIONALE 2019

LE COMPETENZE... UNA RISORSA PER LE PERSONE, IL LAVORO, LA SOCIETA'

La cogenza del Regolamento EU 679/16 (GDPR) nei Sistemi di Gestione

Relatore: Attilio Rampazzo

Milano, 11 Ottobre 2019
Roma, 18 Ottobre 2019

Sommario

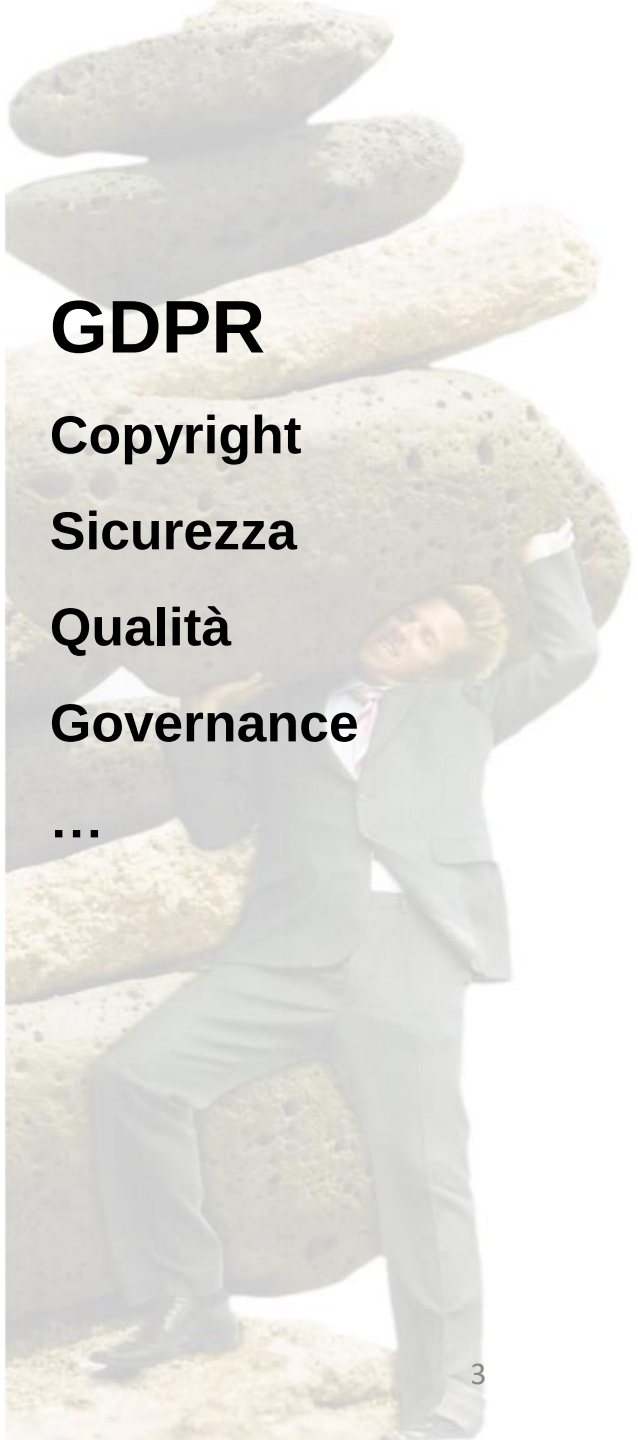
- Scenario
- Alcuni termini e definizioni
  - Cos'è la *compliance*?
  - Cos'è il GDPR?
  - Cos'è un Sistema di Gestione?
- GDPR vs Sistemi di Gestione
- Legame GDPR vs Sistemi di Gestione
- Audit Sistema di Gestione vs GDPR

Scenario

Le Organizzazioni si trovano, nell'attuale panorama competitivo, sempre più a dover affrontare sfide complesse:

- Mercato
- Cambiamenti
- Conoscenze (Sapere)
- Situazione economica
- Clientela
- ***Compliance*** **(norme e leggi)**
- … … …

Si rendono pertanto necessarie scelte organizzative che sono condizionate da queste sfide



Che cos'è la *compliance*?

In campo economico ed organizzativo con il termine **compliance normativa** (o *regulatory compliance*, in italiano anche **conformità normativa**) si intende la conformità a determinate norme, regole o standard.

Nelle Organizzazioni, la ***compliance* normativa** indica il rispetto di specifiche disposizioni impartite dal legislatore, da autorità di settore nonché di regolamentazioni interne alle Organizzazioni stesse.

Che cos'è il GDPR?

A fare il massimo ritenuto adeguato **dal Titolare e Responsabile** sulla base della **valutazione del proprio trattamento** e del relativo **rischio e impatto**

Dando **prova** che le soluzioni adottate siano le misure tecniche e organizzative adeguate al caso concreto

Da fare il minimo previsto dalla legge

E' il principio dell'**Accountability**

Che cos'è un Sistema di Gestione?

Un Sistema di Gestione (SG) è un insieme di processi, regole e procedure, definito in una norma riconosciuta a livello internazionale, che un'Organizzazione può applicare allo scopo di raggiungere obiettivi definiti, quali ad esempio:

- la **soddisfazione** del cliente
- il **miglioramento continuo** delle prestazioni dell'Organizzazione
- la capacità di **dimostrare** a terzi (ossia a clienti o potenziali clienti, organismi di controllo, fornitori o altri soggetti esterni all'Organizzazione) la propria **affidabilità** nel mantenere con **continuità** i propri impegni e **soddisfare sempre i requisiti dei clienti e cogenti (leggi e regolamenti).**

L'obiettivo generalmente è quello di **attuare strumenti che consentono all'Organizzazione di tenere sotto controllo i propri processi e le proprie attività**.

L'adozione di un Sistema di Gestione è volontaria e un Organismo Terzo, se richiesto, deve certificare la sua efficacia e la sua conformità.

GDPR vs Sistemi di Gestione

La norme specificano i **requisiti** di un Sistema di Gestione quando un'Organizzazione desidera accrescere la soddisfazione delle esigenze della propria utenza tramite l'applicazione efficace del Sistema, a partire dai processi per il miglioramento continuo del Sistema, e l'assicurazione della **conformità** sia ai requisiti richiesti dall'utenza che imposti dalle norme applicabili, legali e contrattuali (**requisiti cogenti**).

GDPR è un requisito cogente!

GDPR vs Sistemi di Gestione

Nel caso del GDPR, o Regolamento UE 679/2106, si tratta di una **cogenza** importante che ogni Organizzazione deve adempiere per rispettare la legislazione europea.

Diverso è il criterio con cui tale Regolamento possa o meno essere considerato una delle cogenze di prodotto/servizio ai fini di una certificazione ISO 9001 o dei requisiti ai fini della certificazione ISO/IEC 27001 od altre norme.

GDPR vs Sistemi di Gestione

Il GDPR 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.

GDPR vs Sistemi di Gestione

UNI EN ISO 9001:2015

Sistemi di gestione per la qualità - Requisiti

Scopo e campo di applicazione

La presente norma internazionale specifica i requisiti di un Sistema di Gestione per la Qualità quando un'Organizzazione:

a) 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; e

b) mira ad accrescere la soddisfazione del cliente tramite l'applicazione efficace del Sistema, compresi i processi per migliorare il sistema stesso e assicurare la conformità ai requisiti del cliente e ai **requisiti cogenti** applicabili.

Nota 2: È possibile che i requisiti cogenti siano espressi come requisiti legali.

Nota Nazionale - Per "requisiti cogenti" si intendono, nel seguito, l'insieme dei requisiti obbligatori, in particolare i requisiti legislativi (*statutory*) e regolamentari (*regulatory*) di cui alla ISO 9000:2015, punti 3.6.6 e 3.6.7.

UNI CEI ISO/IEC 20000-1:2014

Tecnologie informatiche - Gestione del servizio - Parte 1: Requisiti per un sistema di gestione del servizio

4.5.2 Pianificare il SGS (Plan)

… …

d) le politiche, le norme, le **prescrizioni legali e regolamentari**, e gli obblighi contrattuali;

6.6.1 Politica della sicurezza delle informazioni

La direzione avente appropriata autorità deve approvare una politica per la sicurezza delle informazioni, prendendo in considerazione i requisiti del servizio, **le prescrizioni legali e regolamentari** e gli obblighi contrattuali.

… …

ISO/IEC 20000-1:2018

Information technology — Service management — Part 1: Service management system requirements

4.2 Understanding the needs and expectations of interested parties

… …

NOTE The requirements of interested parties can include service, performance, **legal and regulatory requirements** and contractual obligations that relate to the SMS and the services.

6.3 Plan the service management system

… …

c) obligations such as relevant policies, standards, **legal, regulatory and contractual requirements**, and how these obligations apply to the SMS and the services;

UNI CEI EN ISO/IEC 27001:2017

Tecnologie informatiche - Tecniche per la sicurezza - Sistemi di gestione per la sicurezza delle informazioni - Requisiti

4.2 Comprendere le necessità e le aspettative delle parti interessate

Nota I requisiti delle parti interessate possono includere **requisiti cogenti** e obblighi contrattuali.

Nota nazionale - Per "requisiti cogenti" si intendono, nel seguito, quelli stabiliti da leggi, regolamenti, direttive (requisiti legali) e prescrizioni obbligatorie in genere.

APPENDICE A OBIETTIVI DI CONTROLLO E CONTROLLI DI RIFERIMENTO

A.18.1 Conformità ai requisiti cogenti e contrattuali

Obiettivo: Evitare violazioni a **obblighi cogenti** o contrattuali relativi alla sicurezza delle informazioni e di qualsiasi requisito di sicurezza.

ISO/IEC 27701:2018

Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines

6.15 Compliance

6.15.1 Compliance with legal and contractual requirements

6.15.1.1 Identification of applicable legislation and contractual requirements

The control, implementation guidance and other information stated in ISO/IEC 27002:2013, 18.1.1 and the following additional guidance applies:

Additional other information for 18.1.1, Identification of applicable legislation and contractual requirements, of ISO/IEC 27002:2013 is:

The organization should identify any potential legal sanctions (which can result from some obligations being missed) related to the processing of PII, including substantial fines directly from the local supervisory authority. In some jurisdictions, International Standards such as this document can be used to form the basis for a contract between the organization and the customer, outlining their respective security, privacy and PII protection responsibilities. The terms of the contract can provide a basis for contractual sanctions in the event of a breach of those responsibilities.

UNI EN ISO 22301:2014

Scopo e campo di applicazione

… …

Queste esigenze sono modellate da **requisiti cogenti**, regolamentari, dell'Organizzazione stessa e del settore industriale di riferimento, dai prodotti e servizi, dai processi utilizzati, dalla dimensione e struttura dell'Organizzazione, e dai requisiti delle relative parti interessate.

8.2 Analisi di impatto sul business e valutazione dei rischi

… …

b) tenga conto dei **requisiti legali** e di altro tipo, a cui l'organizzazione deve sottostare,

… …

GDPR vs Sistemi di Gestione

Chi ha attivato un Sistema di Gestione funzionante 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**.

GDPR vs Sistemi di Gestione

Una breve carrellata di documenti da verificare relativamente al rispetto del GDPR (elencazione non esaustiva):

- Registro dei Trattamenti;
- 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 ed 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 …);
- Sistema di verifiche (audit interni) sul rispetto del Regolamento UE 679/16;
- Modalità di *privacy by design* e *by default*

Chi deve essere adeguato

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 di 3° parte deve sicuramente essere verificata l'applicazione del GDPR

- 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";
- imprese di somministrazione di lavoro e ricerca del personale;
- società operanti nel settore della cura della salute, della prevenzione/diagnostica sanitaria;
- società di call center;
- società che forniscono servizi informatici;
- società che erogano servizi televisivi a pagamento.

Audit Sistema Gestione vs GDPR

E’ 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
- la rilevanza dei requisiti cogenti di prodotto/servizio secondo la ISO 9001 oppure i controlli od obiettivi della ISO/IEC 27001 sulla conformità … …

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.

Audit Sistema Gestione vs GDPR

E’ importante pertanto definire il livello d’indagine che spetta ad un Auditor di un Organismo di Certificazione in merito al rispetto dei citati **requisiti cogenti**.

Da ciò emerge una riflessione importante che impone agli auditor dei Sistemi di Gestione, 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.

Audit Sistema Gestione vs GDPR

Resta importante tenere aperto il dibattito

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 Sistema di Gestione con il GDPR/Regolamento UE 679/2016.

Per far questo è necessario offrire al mercato un sistema di misura e di valutazione delle professionalità credibile e qualificato.

Audit Sistema Gestione vs GDPR

Riferimenti:

- Newsletter AICQ SICEV nr. 3/2019 scaricabile dal sito

Grazie per l’attenzione