Dal 25 maggio 2018 è divenuto pienamente applicabile in tutti gli Stati membri [il **Regolamento Ue 2016/679**,](https://www.agendadigitale.eu/infrastrutture/nuovo-regolamento-privacy-ue-ecco-tutto-cio-che-cittadini-e-pa-devono-sapere/) noto come **GDPR** (General Data Protection Regulation) **–** relativo alla protezione delle persone fisiche con riguardo al **trattamento e alla libera circolazione dei dati personali**.

Applicare il GDPR (General Data Protection Regulation) significa far entrare nell’operatività quotidiana delle aziende anche la gestione del dato personale . Quindi non si dovrebbe vedere l’applicazione del Regolamento Europeo come un qualcosa di burocratico, , ma come un processo vero e proprio.

Questo concetto è lo stesso che si attua nei Sistemi di Gestione Qualità (UNI EN ISO 9001:2015).

Ecco perché le aziende che hanno già un Sistema Gestione Qualità possono sfruttare a proprio vantaggio una eventuale integrazione della documentazione privacy all’interno della struttura del Sistema Qualità, che inoltre consente di tenere sotto controllo le revisioni dei documenti.

I processi derivanti da normative, siano esse obbligatori (ad es. il Regolamento Europeo Privacy) o volontarie (ad es. la ISO 9001), devono:

* + essere tenuti sotto controllo;
  + rispettare i requisiti delle normative;
  + integrarsi nel sistema organizzativo aziendale.

Il Sistema di Gestione Qualità è uno standard che definisce i requisiti minimi che un’organizzazione deve avere per:

* + monitorare e misurare le caratteristiche del prodotto
  + verificare che i requisiti siano stati soddisfatti
  + Conservare l’evidenza della conformità ai requisiti.
  + accrescere la soddisfazione del cliente.

Il Regolamento Europeo Privacy **è una norma obbligatoria** che definisce i requisiti minimi che un’organizzazione deve avere per:

* dimostrare la protezione delle persone fisiche con riguardo al trattamento dei dati personali.

I punti di contatto tra la norma UNI EN ISO 9001 ed il GDPR sono

*“L’organizzazione deve mettere a disposizione l’infrastruttura necessaria per l’attuazione del SGQ (par. 7.1.3 della norma ISO 9001)”*, quindi, anche sistemi hw e sw, antivirus, 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 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 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.

*“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.

Ogni Organizzazione che gestisce dati personali e particolari attraverso computer, server, supporti informatici o cartacei trae numerosi vantaggi dall’integrazione di un SGQ con il Regolamento UE 679/2016.

Infatti, in fase di audit ( come previsto nelle norme ISO 9001) saranno controllati anche i documenti relativi ai Trattamento dei dati personali *ricordando che* in caso di controllo/verifica del Garante della Privacy (o Nucleo Speciale Privacy della Guardia di Finanza), comporterebbe sicuramente sanzioni, previste dal Regolamento UE 679/16. Pertanto, sarà compito dell’auditor rilevare eventuali mancanze su tutta la documentazione compresa quella relativa al trattamento dei dati personali definendo la classificazione.