Allegoria del Buon Governo (A. Lorenzetti, 1338): il buon governo ispirato dalle virtù e, tra esse, dalla Temperanza per impegnare saggiamente il tempo e dalla Prudenza per interpretare il passato, leggere il presente e prevedere il futuro.

Progetto RPD
negli Enti pubblici e nelle Società partecipate

Siinnova Consulting

00137 Roma - Via Isidoro del Lungo, 28

Tel. 06/87463009 Fax 06/80691738

www.siinnova-consulting.it – mail to: info@siinnova-consulting.it – siinnova-consulting@pec.it

Il D.lgs. 101/18: le responsabilità introdotte

Con il D.lgs. 181/18, in vigore dal 19 settembre 2018, il Legislatore, recependo, in via definitiva, il regolamento europeo (General Data Protection Regulation – GDPR - UE 2016/679), ha inteso investire gli Enti pubblici di nuove responsabilità in relazione alla gestione dei dati personali raccolti, di norma in quantità rilevanti, per finalità di pubblico interesse.

La gestione dei dati in modo lecito, corretto e trasparente deve sottendere un approccio proattivo attraverso cui valutare, verificare e correggere il trattamento ancor prima che esso avvenga; il titolare del trattamento, sin dalla fase di pianificazione e progettazione di un servizio o di un'attività, si occuperà di organizzare la raccolta, conservazione ed utilizzo dei dati con un livello di protezione conforme ai requisiti normativi.

La responsabilità del titolare, estesa altresì a tutti i responsabili del trattamento delegati, è inoltre correlata alla puntuale rendicontazione (accountability) di quanto realmente attuato, sia sotto il profilo organizzativo che gestionale, per mitigare soddisfacentemente il rischio di illecito trattamento di dati personali, anche accidentale, che sia lesivo dei diritti e libertà dei cittadini.

Il D.lgs. 101/18: le sanzioni

***L'art. 166 del nuovo Codice Privacy prevede sanzioni minori (fino a 10 milioni di euro** o al 2% del fatturato dell'Organizzazione) **e maggiori (fino a 20 milioni di euro** o al 4% del fatturato dell'Organizzazione) in caso di violazioni, tra le altre, delle disposizioni relative a:*

- **informativa da rendere con linguaggio semplificato ai minori di quattordici anni e/o raccolta del consenso in occasione dell'offerta diretta di servizi della società dell'informazione;**
- **trattamento per l'esecuzione di un compito di interesse pubblico che presenta rischi elevati;**
- **trattamento di particolari categorie di dati per motivi di interesse pubblico rilevante;**
- **trattamento ed informazione resa dai fornitori di reti pubbliche di comunicazioni o di servizi di comunicazione elettronica accessibili al pubblico;**
- **trattamento a fini statistici e di ricerca scientifica;**
- **trattamento nell'ambito dei rapporti di lavoro;**
- **valutazione di impatto per specifici trattamenti e particolari tipologie di dati;**
- **regole deontologiche promosse dal Garante;**
- **misure di garanzia per il trattamento di dati genetici, biometrici e relativi alla salute;**
- **richiesta di informazioni ed esibizione di documenti.**

Il D.lgs. 101/18: le sanzioni

Le sanzioni sono decise e comminate dal Garante per la Protezione dei Dati Personali sulla base del singolo caso; la decisione sull'imposizione delle sanzioni e della relativa quantificazione sottende la valutazione di fattori quali :

- **natura, gravità e durata della violazione**
- **intenzionalità o semplice negligenza della violazione**
- **categorie di dati personali interessati, numero di interessati ed impatto su di essi**
- **misure attuate per proteggere i dati ed aderenza alle norme cogenti**
- **eventuali infrazioni precedentemente commesse.**

Alla sanzione amministrativa è da aggiungere l'eventuale risarcimento richiesto dagli interessati.

Le sanzioni penali (artt. 167, 168, 170, 171 e 172 del Codice) riguardano:

- **trattamento illecito di dati**
- **comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala**
- **acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala**
- **falsità nelle dichiarazioni e interruzione dell'esecuzione di compiti o dell'esercizio di poteri del Garante**
- **inosservanza dei provvedimenti del Garante**
- **violazione delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori.**

Il nuovo Codice ha abrogato il reato di cui al previgente art. 169, relativo alle misure di sicurezza.

Il quadro normativo: i principi cardine alla base del trattamento

I principi cardine alla base del trattamento sono :

- liceità, correttezza e trasparenza nei confronti dell'interessato:

➡ dati trattati esclusivamente alle condizioni previste dal Regolamento;

- limitazione delle finalità della raccolta dei dati:

➡ raccolti per finalità determinate e trattati secondo modalità compatibili con tali finalità;

- minimizzazione dell'uso dei dati:

➡ adeguati e pertinenti a quanto necessario per il perseguimento delle relative finalità;

- esattezza dei dati:

➡ esatti e aggiornati, con la cancellazione di quelli inesatti;

- limitazione della conservazione

➡ conservati per il solo tempo necessario al raggiungimento delle finalità previste.

Il Regolamento introduce poi i concetti di privacy by design e by default: la protezione dei dati diventa essa stessa un principio cardine dovendo essere assicurata fin dalla progettazione dei sistemi di trattamento; inoltre, per impostazione predefinita, i sistemi devono trattare esclusivamente i dati personali necessari per ogni specifica finalità.

Le figure: il Responsabile della protezione (RPD)

- Gli Enti Pubblici devono nominare il Responsabile della protezione dei dati personali [RPD o Data Protection Officer – DPO], secondo l'art. 37 del Regolamento (UE) 2016/679.
- Il RPD è un soggetto designato dal titolare o dal responsabile del trattamento per assolvere a funzioni di supporto e controllo, consultive, formative e informative relativamente all'applicazione del Regolamento GDPR. Coopera altresì con l'Autorità e costituisce il punto di contatto, anche rispetto agli interessati, per le questioni connesse al trattamento dei dati personali (artt. 38 e 39 del Regolamento).
- E' una figura anche esterna all'Organizzazione – persona fisica o giuridica – cui non si richiedono specifiche attestazioni formali o l'iscrizione in appositi Albi bensì, oltre ad un'imprescindibile conoscenza della normativa:
  - capacità consulenziali e competenze organizzative;
  - competenze nella disciplina del risk assessment & management;
  - conoscenze dei sistemi informativi/informatici e delle tecnologie per la protezione dei dati;
  - abilità nella formazione del personale e nell'esecuzione di audit;
  - attitudini relazionali e capacità di problem solving,

assicurando altresì che eventuali altri compiti e funzioni assunti non siano in conflitto di interessi con l'incarico di Responsabile della protezione, figura assolutamente indipendente all'interno dell'Ente.

Le figure: il Responsabile della protezione (RPD)

Il RPD adempie alle seguenti mansioni:

- ☑ *informare e fornire consulenza al titolare e/o al responsabile del trattamento nonché ai dipendenti impegnati nel trattamento di dati in merito agli obblighi derivanti dal Regolamento e da altre disposizioni normative cogenti;*
- ☑ *monitorare l'osservanza del GDPR, delle altre disposizioni nonché delle politiche adottate dal titolare o dal responsabile del trattamento, comprese l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle correlate attività di controllo;*
- ☑ *fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;*
- ☑ *cooperare con l'autorità di controllo e fungere da punto di contatto con essa per questioni correlate al trattamento, tra cui la consultazione preventiva;*
- ☑ *partecipare regolarmente alle riunioni del management sui temi della protezione dei dati;*

Le figure: il Responsabile della protezione (RPD)

Il RPD adempie alle seguenti mansioni:

- ☑ *fornire consulenze qualificate ogniqualvolta debbano essere assunte decisioni che impattano sulla protezione dei dati;*
- ☑ *effettuare analisi approfondite qualora si verifichino violazioni dei dati (data breach) o altri incidenti;*
- ☑ *effettuare, su delega del titolare, la valutazione d'impatto sulla protezione ei dati (DPIA);*
- ☑ *tenere, su delega del titolare i registri delle attività di trattamento e quelli relativi alla violazione dei dati (data breach);*
- ☑ *fornire le necessarie informazioni ed attivare ogni comunicazione con l'Autorità garante e con gli interessati del trattamento.*

Il "Progetto RPD": l'intervento proposto

Siinnova Consulting, *forte dell' esperienza ultraventennale maturata dai propri consulenti e formatori nell'ambito dei modelli di compliance in settori merceologici, pubblici e privati, i più diversificati in relazione a quanto previsto dal D.Lgs. 101/18 di adeguamento alle disposizioni del Regolamento (UE) 2016/679, offre la propria consulenza ed assistenza per gli adempimenti normativi richiesti.*

L'intervento, nella prima fase - consulenziale -, si sviluppa attraverso le seguenti fasi (alcune qualora delegate dal titolare del trattamento):

- *valutazione e **quantificazione dei rischi e degli impatti derivanti dal trattamento dei dati**, soprattutto sensibili, ed eventuale formalizzazione delle risultanze, qualora se ne rilevi l'obbligo;*
- *individuazione ed **analisi degli aspetti critici**, sia afferenti alla gestione ed ai sistemi info-telematici che all'organizzazione;*
- *rivisitazione delle **informative agli interessati** e delle modalità per le **richieste di autorizzazione, negazione o revoca del consenso** al trattamento dei dati;*
- *definizione degli **interventi finalizzati a mitigare i rischi di violazione** dei dati ed ad ottimizzare i processi di trattamento, anche nella logica di migliorare l'accountability;*
- *individuazione delle modalità di intervento e delle **procedure di sicurezza in caso di eventuali violazioni e/o perdite di dati** (cd. digital disruption e data breach);*
- *individuazione delle **tecnologie info-telematiche e delle procedure organizzative finalizzate a proteggere i dati trattati da attacchi o perdite**, anche accidentali, sia attraverso misure di prevenzione (riducendo la probabilità di accadimento dell'evento indesiderato) che di protezione (riducendo la gravità del danno conseguente).*

Il "Progetto RPD": l'intervento proposto

L'intervento, nella seconda fase - assistenziale -, prevede il coinvolgimento di un consulente cui è affidato, su nomina e delega del titolare del trattamento, l'incarico di Responsabile della protezione dei dati (RPD) con i seguenti compiti:

- *promuovere l'attuazione e l'applicazione delle politiche di protezione dei dati, definite congiuntamente al titolare, a tutti i livelli dell'Organizzazione;*
- *indirizzare, coordinare e verificare ogni adempimento previsto dalle normative cogenti;*
- *verificare, puntualmente, sistematicamente e con riferimento a quanto previsto dalle normative, che il trattamento dei dati contempli un'esaustiva informazione all'interessato ed il diritto, quando applicabile, alla negazione o alla revoca del consenso;*
- *monitorare le eventuali violazioni e/o perdite di dati (data breach) e provvedere alla relativa registrazione, notifica al Garante e comunicazione alle parti interessate (qualora coinvolte);*
- *fornire pareri ed indicazioni al titolare del trattamento in merito alla valutazione d'impatto sul trattamento dei dati (DPIA);*
- *fungere da punto di contatto con l'Autorità garante e collaborare con essa per questioni connesse al trattamento e fornire ogni assistenza agli interessati;*
- *provvedere alla tenuta ed aggiornamento dei registri delle attività di trattamento e delle eventuali violazioni di dati;*
- *condividere i verbali e/o gli altri documenti emessi e/o ricevuti nell'ambito della cooperazione con l'Autorità garante per le questioni connesse al trattamento dei dati;*
- *vigilare sugli obblighi derivanti dal GDPR e sul corretto adempimento a tutti i livelli dell'Organizzazione.*

Il "Progetto RPD": l'intervento proposto

Siinnova Consulting ***offre l'esperienza e competenza dei propri consulenti e formatori per assolvere a tutti gli adempimenti previsti dal Regolamento GDPR, così come recepito dal D.Lgs. 101/18 del 10/08/18, compresa la nomina e la concreta operatività del Responsabile della protezione dei dati, anche con l'intento di fornire consulenza ed assistere proficuamente il titolare ed i responsabili del trattamento nominati in seno all'Ente.***