Allegato 2 alla Disposizione n. 40 del 01 Ottobre 2018

Indicazioni operative per Linee Guida Organizzazione Ente

Versione del documento	1.4
Data emissione	01/10/2018
Stato del documento	Bozza
Nome del file	"Indicazioni operative per Linee Guida Organizzazione Ente.docx"

Sommario

1 Contesto di riferimento

La presente introduzione è necessaria al fine di inquadrare sotto un profilo contestuale il Regolamento Europeo nr. 679/2016 (General Data Protection Regulation meglio noto come GDPR), entrato in vigore il 24 maggio 2016 ma pienamente applicabile a partire dal 25 maggio 2018, che andrà ad uniformare ed armonizzare le legislazioni dei Paesi Europei con riguardo alla materia di protezione dei dati personali.

L'esigenza di una rivisitazione della normativa in materia di protezione dei dati personali si apprezza in relazione al mutato contesto politico, economico e sociale di riferimento del tutto differente rispetto a quello degli anni 90, periodo nel quale l'impatto e la cultura del dato non era così centrale come invece è oggi; ciò è dato dallo sviluppo repentino delle moderne tecnologie (in primis mobile devices, smartphone, tablet, social network, ecc.; in seconda battuta strumenti IOT (Internet of things), sistemi di Data Analytics e Big Data, Business Intelligence, ecc.) nemmeno immaginabile negli anni che chiudevano il secolo scorso, grazie alle quali è pensabile e apprezzabile anche il valore economico del dato.

Accanto a questa constatazione di tipo "sociologica" va da sé che il programma di integrazione europeo che vede come base di partenza la creazione di un mercato unico europeo, da realizzarsi inizialmente attraverso la libera circolazione di persone, servizi e merci, non possa non tenere in considerazione anche della libera circolazione del "dato personale" così come puntualmente sottolineato dai "considerando" del Regolamento fino anche alla maggiore rilevanza di questa libertà rispetto alla tutela del dato in sé come diritto soggettivo (considerando nr. 4).

A seguito di questa breve introduzione storica/sociologica ed avviando la riflessione sul terreno giuridico, in prima battuta preme precisare che la scelta di tipologia di intervento del legislatore Europeo risulta alquanto significativa nella misura in cui, con la scelta di un Regolamento, non viene lasciata agli Stati membri alcuna possibilità di intervento (se non in termini di adozione di provvedimenti volti ad armonizzare la normativa nazionale) stante la piena applicabilità del Regolamento a dispetto della presenza, come successo invece in passato in materia di protezione di dati personali, di direttiva europea (95/46) che necessitava di un atto di recepimento (Dlgs. 196/2003, meglio noto come codice della privacy).

In riferimento invece ai contenuti della presente legge si sottolinea come l'approccio che propone il Regolamento sia del tutto differente rispetto a quello proposto dal codice privacy nazionale.

Principio fondamentale che impernia l'intera normativa è infatti quello di **accountability** (la capacità di rendere conto delle azioni) il quale illustra, di fatto, una responsabilizzazione dei soggetti coinvolti in materia di protezione di dati personali; questi infatti secondo il dettato normativo non dovranno più ragionare in termini di mero adempimento alla norma di riferimento, come invece accaduto fino ad oggi con riferimento ai dettami del codice della privacy.

In tal senso il principio di accountability deve essere letto sotto un duplice profilo: esso non solo è il principio che ispira l'adeguamento/l'adempimento degli enti alla normativa europea, ma è anche il punto di partenza per **dimostrare** la compliance (il rispetto, l'aderenza) dell'ente/organizzazione alla norma europea.

Ciò significa che un ente/organizzazione può disattendere una prescrizione del Regolamento, avendo tuttavia cura di indicare in apposito documento le ragioni in forza delle quali si ritiene di non dover seguire il dettato normativo.

Oltre quindi a lasciare uno spazio di intervento ai soggetti Titolari del trattamento in ordine alla scelta di adozione delle novità introdotte dal GDPR, obbligandoli comunque ad una seria riflessione in ordine alle politiche da adottare per essere conformi al Regolamento, si segnalano a titolo esemplificativo alcuni istituti del tutto lontani dalla logica "burocratica" del Codice Privacy.

Si richiama inevitabilmente quindi al processo di istituzione e conservazione del **registro di trattamenti** in capo ai titolari e responsabili del trattamento che consente quindi di avere una chiara panoramica dei trattamenti di dati personali che vengono effettuati all'interno dell'organizzazione che fa per l'appunto capo al titolare o al responsabile; a ciò si aggiunga l'organizzazione del processo che porta il titolare o responsabile del trattamento, in contatto con l'autorità garante e con i soggetti interessati in caso di "violazione di dati" nota anche come **Data Breach,** che come sarà meglio trattato nell'apposito documento non si limita al solo furto di dati.

Ancora, la previsione di una conduzione di **Valutazione di impatto** per quei trattamenti che presentino un rischio elevato per i diritti e le libertà degli interessati.

Sotto il profilo dei soggetti attivi e protagonisti, in questo nuovo quadro, viene introdotta la figura del **Data Protection Officer – DPO** (obbligatorio per tutti gli enti pubblici) il quale si andrà a configurare da un lato come consulente per i Titolari e i Responsabili dei trattamenti, attraverso una continua verifica della compliance dell'organizzazione/ente rispetto ai dettami del GDPR, ma anche come punto di riferimento per i soggetti interessati rappresentando per questi ultimi il referente dell'organizzazione con il quale interfacciarsi in materia di protezione dei dati personali.

In conclusione, come già emerso dalla disamina condotta, a mutare è l'atteggiamento della normativa rispetto alla tematica della protezione dei dati personali, esso infatti impone una riflessione preventiva rispetto alla materia de qua, che porta quindi ad adattare la propria organizzazione in base alle opportunità che si intendono cogliere, lasciando non solo ampi spazi di autonomia ai soggetti Titolari/Responsabili ma anche abbandonando quell'approccio di mero adempimento richiesto dalla normativa. In sintesi, non è sufficiente avere "le carte a posto".

2 Premessa

2.1 Oggetto e obiettivo del documento

Il GDPR riforma il precedente impianto normativo in materia di protezione dei dati personali – Codice Privacy, inserendo come elementi cardine il principio di Accountability o Responsabilizzazione in capo al Titolare, e di eventuali Responsabili o Contitolari del trattamento, nell'adozione di misure tecniche ed organizzative adeguate ed efficaci, con l'onere di dimostrare la conformità delle attività di trattamento al GDPR stesso, garantendo la tutela ai diritti dell'interessato, nonché mettendo in atto procedure per riesaminare e aggiornare le misure stesse.

In tale contesto assume rilievo il cambio di approccio al "tema privacy" da parte del Titolare del trattamento, oggi chiamato a rimodulare i processi di flusso dei dati personali secondo **i principi di privacy "by design" e "by default"**, per avere la certezza che le misure tecniche e organizzative siano adottate ed integrate fin dall'inizio del trattamento; per valutare i rischi che possono violare i dati personali o la tutela della vita privata (come riporta l'art. 1 § 2 del GDPR "il presente regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali"); per priorizzare gli interventi, per avere la garanzia della liceità del trattamento, per monitorare costantemente le misure di sicurezza ed i trattamenti, per rendere i collaboratori consapevoli del valore del dato attraverso la formazione ed infine per garantire che quest'ultimi si impegnino alla riservatezza o che abbiano un adeguato obbligo legale di riservatezza.

Pertanto, diventa prioritaria la riorganizzazione dell'ente/organizzazione cercando di ridistribuire compiti e responsabilità tra i soggetti coinvolti nel trattamento dei dati personali (vedi Titolare del trattamento, Responsabile del trattamento, persona istruita e autorizzata – ex incaricato del trattamento nel codice privacy) con la particolare attenzione di armonizzare il tutto con il nuovo ruolo DPO, introdotto dal GDPR.

Il presente elaborato vuole fornire delle indicazioni generali su come configurare il nuovo assetto organizzativo in materia di protezione dei dati personali e sui requisiti che rendono obbligatorio la designazione del DPO, nonché sulle funzioni e compiti di tale ruolo.

2.2 Ambito di applicazione del documento

Il presente documento ha lo scopo di fornire indicazioni in grado di coadiuvare Regione Toscana e gli Enti ad essa collegati nella definizione delle Linee Guida per l'aggiornamento del Sistema Organizzativo, ai fini dell'applicazione di quanto previsto dal GDPR.

Le presenti indicazioni si applicano a Regione Toscana e a tutti gli Enti che condividono le indicazioni del medesimo DPO come da delibera nr. 325/2018.

2.3 Aggiornamento e validità del documento

2.3.1 Soggetti Approvatori

Approvatore	Referente e Ruolo	Data

2.3.2 Soggetto verificatore

Verificatore	Referente e Ruolo	Data

2.3.3 Versione del documento

Stato	Versione	Autore	Descrizione	Data

3 Quadro normativo

- REGOLAMENTO 2016/679/UE: Articoli 24, 25, 26, 27, 28, 29, 30 e 31
- Considerando C74, C75, C76, C77, C78, C79, C80, C81, C83
- WP 243 rev. 01 - Linee guida sui responsabili della protezione dei dati adottata il 13/12/2016, emendata il 05/04/2017, dal Gruppo di lavoro articolo 29
- WP 169 - Opinion 1/2010 on the concepts of "controller" and "processor" - Adopted on 16 February 2010
- WP 173 - Opinion 3/2010 on the principle of accountability - Adopted on 13 July 2010
- Norma UNI 11697: Attività professionali non regolamentate – Profili professionali relativi al trattamento e alla protezione dei dati personali – Requisiti di conoscenza, abilità e competenza

3.1 Definizioni normative di riferimento

DPIA: acronimo di Data Protection Impact Assessment (valutazione di impatto sulla protezione dei dati).

Dato personale: 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;

Trattamento: 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;

Limitazione di trattamento: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

Profilazione: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

Pseudonimizzazione: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

Archivio: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

Titolare del trattamento o suo delegato: 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 essere stabiliti dal diritto dell'Unione o degli Stati membri;

Responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

Contitolare: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, insieme ad altri determina le finalità e i mezzi di trattamento dei dati personali;

Sub responsabile: persona fisica o giuridica designata dal responsabile del trattamento previa autorizzazione scritta del titolare del trattamento;

Destinatario: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

Terzo: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

Consenso dell'interessato: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

Violazione dei dati personali: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

Dati biometrici: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

Dati relativi alla salute: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

Security Manager: si tratta della figura preposta alla gestione e supervisione del processo di Security Incident Management.

Responsabile della Conservazione documentale: si tratta della figura preposta alla gestione e supervisione del processo di conservazione dei documenti (digitali o cartacei).

Autorità di controllo: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51.

Rappresentante: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del regolamento;

Misure di sicurezza: misure tecniche ed organizzative adeguate per garantire un livello di sicurezza dei dati trattati adeguato al rischio.

Anonimizzazione: tecnica di trattamento dei dati personali tramite la quale i dati personali non possano più essere attribuiti a un interessato specifico, nemmeno attraverso l'utilizzo di informazioni aggiuntive.

Cifratura: tecnica di trattamento dei dati personali tramite la quale i dati personali vengono resi non intellegibili a soggetti non autorizzati ad accedervi.

Data Breach: incidente di sicurezza in cui i dati personali, vengono consultati, copiati, trasmessi, rubati o utilizzati da un soggetto non autorizzato o persi accidentalmente.

Interessato: persona fisica identificata o identificabile. 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.

Nuovo trattamento: trattamento di dati personali che comporta l'utilizzo di nuove tecnologie o è di nuovo tipo e in relazione al quale il titolare del trattamento non ha ancora effettuato una valutazione d'impatto sulla protezione dei dati, o la valutazione d'impatto sulla protezione dei dati si riveli necessaria alla luce del tempo trascorso dal trattamento iniziale.

Privacy by-design / by-default: l'incorporazione della privacy a partire dalla progettazione di un processo aziendale, con le relative applicazioni informatiche di supporto. La prima introduce la protezione dei dati fin dalla progettazione per caso specifico, la seconda per impostazione predefinita di una pluralità di casi tra loro omogenei.

3.2 Sistema organizzativo previsto dalla normativa

3.2.1 Approccio di responsabilizzazione sostanziale

In riferimento alle specifiche novità introdotte dal GDPR – così come evidenziato in precedenza - si determina un approccio di responsabilizzazione sostanziale, con l'espressa indicazione di una privacy

compliance basata su metodologie di valutazione del rischio e che deve essere integrata nei processi dell'Ente.

In altri termini, il Regolamento impone un "approccio preventivo, proattivo e non più reattivo", con focus su obblighi e comportamenti che prevengano in modo effettivo il possibile evento di danno, configurandosi sulle specificità dei diversi trattamenti cui si riferiscono.

Tutto ciò lo aveva già chiarito esplicitamente un parere (Opinion 3/2010 – WP art.29) espresso dal Gruppo di Lavoro Articolo 29, significativamente intitolato "*Opinion 3/2010 on the principle of accountability*" laddove si è, tra l'altro, raccomandato che **il titolare del trattamento dei dati debba essere in grado di *dimostrare di avere adottato un processo complessivo di misure giuridiche, organizzative, tecniche, per la protezione dei dati personali, anche attraverso l'elaborazione di specifici modelli organizzativi*** **e che debba *dimostrare in modo positivo e proattivo che i trattamenti di dati effettuati sono adeguati e conformi al regolamento europeo in materia di privacy*.**

3.2.2 Titolare del trattamento

Lo sviluppo delle considerazioni riportate nel paragrafo precedente ha poi generato la previsione specificamente contenuta nell'art. 24 del Regolamento 2016/679, rubricato "**Responsabilità del titolare del trattamento**" in cui, per l'appunto, è previsto che, il titolare del trattamento metta *in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento sia effettuato conformemente al presente regolamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.*

In questo quadro, si delinea un sistema organizzativo ai fini dell'applicazione del GDPR in cui il Titolare assume il ruolo principale attore del sistema del trattamento. Come indicato dal considerando n.74, il Titolare del trattamento assume la **responsabilità generale** per qualsiasi trattamento di dati personali che effettui direttamente o che altri abbiano effettuato per suo conto.

Infatti, l'art. 5 del GDPR attribuisce direttamente ai titolari del trattamento il compito di assicurare, ed essere in grado di comprovare, il rispetto dei principi applicabili al trattamento dei dati personali.

Il titolare per rispettare il principio di accountability deve assicurare che i dati siano sempre:

- trattati secondo "liceità, correttezza e trasparenza"
- raccolti per "finalità determinate, esplicite e legittime"
- adeguati, pertinenti e limitati rispetto alle finalità
- esatti
- limitati nella conservazione

- trattati garantendo sicurezza e integrità.

Per l'individuazione del titolare si deve fare riferimento – in base a quanto previsto dall'art. 4 del GDPR – alla "persona giuridica, autorità pubblica, servizio o di altro organismo" che determina le finalità e i mezzi del trattamento di dati personali.

Con riferimento ad un Ente, va specificato che la necessaria identificazione della "persona giuridica, autorità pubblica, servizio o di altro organismo" quale titolare o contitolare del trattamento non preclude l'applicazione dei principi generali in materia di formazione della volontà dell'ente e di delega di funzioni, nel senso che la volontà del "titolare/contitolari" sarà formata, anche agli effetti della disciplina della protezione dei dati, tenendo conto delle ordinarie attribuzioni degli organi previsti dall'atto costitutivo e dallo statuto.

In tal senso, sono da considerare - per ogni Ente - tutte le caratteristiche specifiche che influiscono sul processo di determinazione delle finalità e dei mezzi del trattamento di dati personali.

Nel caso di una Pubblica Amministrazione, ai fini dell'individuazione del Titolare va inoltre considerato che le ripartizioni di competenze sono stabilite da norme specifiche e non da provvedimenti amministrativi.

In merito, l'articolo 97 della Costituzione dispone che "I pubblici uffici sono organizzati secondo disposizioni di legge, in modo che siano assicurati il buon andamento e l'imparzialità dell'amministrazione. Nell'ordinamento degli uffici sono determinate le sfere di competenza, le attribuzioni e le responsabilità proprie dei funzionari".

Ogni soggetto pubblico ha per legge specifiche attribuzioni stabilite dalla legge, distinte dalle competenze che fanno riferimento agli organi dell'Ente (quali Consiglio, Giunta, Presidente della Giunta).

Quindi, vista la riserva di legge posta dall'art. 97 Costituzione, non è possibile trasferire la competenza da un organo ad un altro con un provvedimento amministrativo, ma l'autorità amministrativa competente può trasferire l'esercizio di proprie competenze ad un altro organo mediante la delega, così che – senza incidere sulla titolarità delle competenze – si determina lo spostamento dell'esercizio delle stesse.

In altri termini, tramite la soluzione amministrativa della Delega di funzioni un organo può delegare alcune attività ad un altro organo, senza per questo spossessarsi delle proprie sfere di competenza.

Tuttavia, per poter avvalersi di tale soluzione è necessario che lo statuto e la regolamentazione applicabile all'Ente in materia di organizzazione e di ordinamento del personale consentano espressamente all'organo la facoltà dell'esercizio della delega di funzioni.

In caso il modello organizzativo dell'Ente preveda che un organo possa esercitare i poteri delegati da un altro organo (e nello specifico, dall'organo amministrativo collegiale), a tale organo possono essere delegate alcune attività del Titolare del trattamento.

In conclusione, le specifiche del modello organizzativo amministrativo adottato dall'Ente costituisce l'elemento qualificante per determinare le scelte della volontà (e le modalità di esercizio delle stesse) di un

Ente attraverso la struttura amministrativa che le compete, incluse quelle relative alle finalità e ai mezzi del trattamento di dati personali.

3.2.3 Data Protection Officer (DPO)

Il Data Protection Officer – DPO –, altrimenti noto come Responsabile della protezione dei dati, è una nuova figura di riferimento, per tutto ciò che attiene la materia di protezione dei dati personali, e si affianca al Titolare o al Responsabile del trattamento e nei rapporti esterni con le Autorità di controllo e con gli Interessati.

Il DPO è una figura la cui nomina è obbligatoria solo in presenza di determinate condizioni, benché possa essere nominata anche su base volontaria. Si tratta di un obbligo che vige sia in capo ai Titolari che ai Responsabili del trattamento.

Il DPO è parte dell'organizzazione interna del Titolare o del Responsabile del trattamento, quando nominato; ciò nonostante non dovrà necessariamente essere un dipendente dell'azienda o organizzazione ma potrà essere un soggetto esterno che ricopre tale ruolo su incarico del Titolare o del Responsabile del trattamento.

Il Gruppo di lavoro art. 29, costituito da tutti i rappresentanti dei Garanti europei, ha più volte ribadito l'importanza della figura del DPO quale pilastro della responsabilizzazione che agisce quale coordinatore della conformità al GDPR.

Come anticipato la designazione di tale ruolo è obbligatorio, ai sensi dell'art. 37 § 1 del GDPR, quando:

a. *il trattamento è 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;*

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'art. 9 del GDPR, ex dati sensibili, o di dati relativi a condanne penali e a reati di cui all'art. 10 del GDPR.*

Nel regolamento non si rinviene alcuna definizione di "autorità pubblica" o "organismo pubblico". Il Gruppo di lavoro art. 29 ritiene che tale definizione debba essere conforme al diritto nazionale; conseguentemente, sono autorità pubbliche o organismi pubblici le autorità nazionali, regionali e locali ma, a seconda del diritto nazionale applicabile, la nozione ricomprende anche tutta una serie di altri organismi di diritto pubblico, tale per cui, la nomina di un DPO è obbligatoria.

Lo svolgimento di funzioni pubbliche e l'esercizio di pubblici poteri non riguardano esclusivamente le autorità pubbliche e gli organismi pubblici, potendo riferirsi anche ad altre persone fisiche o giuridiche, di

diritto pubblico o privato, in ambiti che variano a seconda delle disposizioni fissate nel diritto interno di ciascuno Stato membro: trasporti pubblici, forniture idriche ed elettriche, infrastrutture stradali, emittenti radiotelevisive pubbliche, istituti per l'edilizia pubblica o organismi di disciplina professionale.

3.2.4 Responsabile del trattamento

Il Regolamento definisce il Responsabile del trattamento come la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare (art. 4, § 8; art. 28)

L'approccio basato sul rischio e misure di accountability del GDPR influenza anche la figura del Responsabile del trattamento, al quale sono assegnati nuovi compiti e che condivide in certa misura le responsabilità del Titolare, in riferimento al risarcimento del danno a terzi, ed è oggetto di autonome sanzioni amministrative.

il Responsabile risponde per danno se non ha adempiuto agli obblighi previsti dal regolamento, ma anche se ha agito senza rispettare le istruzioni del Titolare.

Il Responsabile è soggetto ad un profilo risarcitorio e in caso disattenda le istruzioni al punto da individuare - con i dati che ha ricevuto in affidamento - proprie finalità diventa a sua volta Titolare del trattamento, con conseguente quadro di riferimento - anche sanzionatorio - ben più pesante, rispetto ad una semplice disattenzione o negligenza nel rapporto con le istruzioni da parte del Titolare.

Il Responsabile del trattamento deve presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti previsti dal GDPR e garantisca la tutela dei diritti dell'interessato.

I trattamenti svolti da un Responsabile devono essere disciplinati da un contratto o altro atto giuridico. Il contratto deve stabilire gli elementi essenziali del trattamento di dati personali curato dal Responsabile.

Il contratto formalizza lo "statuto" delle relazioni tra Titolare e Responsabile.

Deve essere in forma scritta (anche in formato elettronico) e deve prevedere almeno questi contenuti obbligatori:

- materia e durata del trattamento
- natura e finalità del trattamento
- tipo di dati personali e categorie di interessati
- obblighi e diritti del titolare del trattamento

In particolare, il titolare deve stabilire per iscritto che il responsabile in base al contratto si impegna a:

a) trattare dati soltanto su istruzione documentata del titolare

b) consentire i trattamenti solo a persone autorizzate con impegno alla riservatezza o che abbiano un adeguato obbligo legale di riservatezza

c) adottare tutte le misure di sicurezza (es. cifratura, pseudonimizzazione, recupero da backup)

d) rispettare le condizioni per ricorrere a un sub-responsabile del trattamento

e) assistere il titolare per dare seguito alle richieste per l'esercizio dei diritti dell'interessato

f) cancellare o restituire tutti i dati e cancellare le copie esistenti

g) mettere a disposizione del titolare le informazioni per dimostrare il rispetto dei suddetti obblighi e consentire le ispezioni

h) assolvere a tutti gli adempimenti richiesti dal GDPR e dalla normativa vigente applicabile ai trattamenti da effettuare in relazione alle attività oggetto del contratto stesso

i) rilasciare una dichiarazione di conformità generale al GDPR.

Inoltre, nel contratto devono essere riportate anche specifiche istruzioni sul trattamento dei dati personali.

A titolo esemplificativo della rilevanza degli impegni contrattuali richiesti, è utile esaminare brevemente le implicazioni degli impegni sopraindicati ai punti b) e f).

In riferimento al punto b) ciò significa che il Responsabile, cui viene affidato il patrimonio informativo del Titolare, deve garantire che le persone (lui stesso e/o suoi eventuali collaboratori) che trattano materialmente quelle basi dati lo facciano attraverso un quadro di assegnazioni di compiti ben puntuale e stabilito perché ne risponde il Titolare nel rapporto con il Responsabile attraverso il contratto.

Riguardo al punto f) si richiede che il responsabile una volta terminato il suo compito contrattuale debba cancellare e restituire tutti i dati e cancellare tutte le copie esistenti: non deve rimanere alcuna traccia dell'affidamento del patrimonio informativo. Deve dare prova di aver cancellato quello che gli è stato affidato e ogni elemento documentale di risulta del trattamento svolto, evitando che si determini una sorta di legame a doppio filo sulle basi dati che renda – di fatto – proprietari i Responsabili, anche successivamente alla conclusione del trattamento.

Il ruolo del Responsabile del trattamento, così come ridefinito dal GDPR, rimanda più alla figura del Responsabile esterno che non a quello interno.

Già un parere (Opinion 1/2010 – WP art.29) espresso dal Gruppo di Lavoro Articolo 29, intitolato *Opinion 1/2010 on the concepts of "controller" and "processor",* indicava che l'esistenza di un responsabile del trattamento dipende da una **decisione** presa dal titolare del trattamento. Quest'ultimo può decidere o di trattare i dati all'interno della propria organizzazione – ad esempio attraverso collaboratori autorizzati a trattare i dati sotto la sua diretta autorità-, o di delegare tutte o una parte delle attività di trattamento a un'organizzazione esterna, cioè a una "**persona giuridicamente distinta dal *titolare* ma che agisce per conto di quest'ultimo**".

In sostanza, ogni qual volta si affida un'attività ad un fornitore esterno e questa attività comporta un trattamento di dati personali si creano i presupposti per la nomina di un Responsabile del trattamento.

3.2.5 Sub-responsabile

Un altro elemento di novità introdotta dal GDPR è la possibilità di designazione da parte del Responsabile di un altro responsabile (c.d. Sub-responsabile del trattamento)

Il Responsabile (c.d. Responsabile primario) può nominare Sub-responsabili per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano titolare e "Responsabile primario".

La nomina dei sub-responsabili può essere effettuata previa autorizzazione scritta (specifica o generale) del titolare.

Il responsabile primario risponde dinanzi al titolare dell'inadempimento del sub-responsabile, anche ai fini del risarcimento di eventuali danni causati dal trattamento.

Nomina sub-responsabili è una facoltà, un'opportunità per semplificare le modalità di trattamento dei dati.

3.2.6 Soggetti istruiti e autorizzati

Nel GDPR non compare il termine Incaricato.

Ai fini di individuare altri soggetti coinvolti nel trattamento dei dati personali, si possono considerare tre elementi, di seguito riepilogati

1. E' definito "terzo" la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia (….) le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del Titolare o del Responsabile (art. 4, § 10)
2. Il Responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del Titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal Titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri. (art. 29)
3. Il Titolare del trattamento e il Responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri (art. 32 § 4).

Quindi per trattare i dati bisogna essere soggetti istruiti e autorizzati. In altri termini, per poter accedere e trattare dati – a qualunque livello di responsabilità diversa da quella del Titolare e del Responsabile – le caratteristiche soggettive e oggettive funzionali richieste consistono nell'essere un soggetto autorizzato che agisce con istruzioni formalizzate dal Titolare del trattamento.

3.3 Ulteriori riferimenti per il sistema organizzativo

3.3.1 Compliance Program

Il Modello organizzativo richiesto dal GDPR rientra nella categoria dei Compliance Program, cioè di modelli organizzativi atti alla prevenzione di rischi di compliance cui è esposto l'Ente.

Per rischio di compliance si intende il rischio di incorrere in sanzioni, subire perdite o danni reputazionali in conseguenza della mancata osservanza di leggi, regolamenti o provvedimenti.

Il Modello per l'applicazione del GDPR, come gli altri Compliance Program, prevede per la propria realizzazione 2 macrofasi:

1) Risk Assessment (identificazione e valutazione dei rischi)
2) Verifica ed eventuale implementazione del Sistema dei controlli (idonei a prevenire i rischi individuati nella macrofase 1).

Il Sistema dei controlli, con riferimento al GDPR, può essere correlato alle misure tecniche e organizzative adeguate a garantire che il trattamento è effettuato in conformità al Regolamento stesso.

Il Sistema dei controlli, o Sistema di controllo interno, in base ai framework di riferimento più diffusi è composto da diversi elementi di controllo generale. Inoltre, le componenti del Sistema di controllo interno devono integrarsi tra loro nel rispetto di una serie di principi di controllo.

Il *Sistema organizzativo costituisce uno degli elementi di rilievo del Sistema di controllo interno*: tener in considerazione le correlazioni del Sistema organizzativo con gli altri componenti del Sistema di controllo interno può consentire di:

- rafforzare la capacità di mitigazione dei rischi delle misure organizzative
- ampliare lo spettro di compensazione/adattamento delle misure organizzative rispetto ad eventuali criticità – temporanee o durature – delle misure tecniche per la prevenzione dei rischi
- favorire un approccio coordinato all'applicazione dei diversi Compliance Program e, conseguentemente, la loro efficacia di prevenzione dei rischi individuati.

3.3.2 Approccio unitario per processi

In riferimento all'approccio di responsabilizzazione sostanziale introdotto dal GDPR si determinano rilevanti ulteriori novità anche in merito al Sistema organizzativo nel suo complesso.

Il Regolamento, come già indicato in precedenza, prevede espressamente una compliance basata su metodologie di valutazione del rischio e che deve essere integrata nei processi dell'Ente.

In altri termini, rispetto al Codice Privacy, si passa dalla richiesta di una somma di adempimenti obbligatori ad un approccio per processi e ad una protezione dei dati personali in ottica Risk Based.

L'approccio per processi favorisce la visione globale dell'organizzazione, rappresentandola attraverso un insieme di processi tra loro interconnessi.

Per un'efficace applicazione del GDPR e del rispetto del principio di accountability, in particolare, è opportuno che il Sistema organizzativo includa la rilevazione dei processi che evidenzi il complesso delle attività svolte, la loro sequenza e le modalità con cui sono corrispondentemente effettuate.

Adempimenti rilevanti ai fini GDPR quali il censimento dei trattamenti dei dati personali, la correlata predisposizione del registro dei trattamenti e il mantenimento dello stesso aggiornato e allineato ad ogni eventuale nuovo trattamento avviato e/o variazione intervenuta nei trattamenti preesistenti implicano che tutte le attività svolte dall'Ente siano analizzate e siano continuamente monitorate.

L'efficacia di tali analisi può essere maggiore se condotta con il supporto preventivo della mappatura dei processi, in modo da poter più facilmente identificare gli ambiti di attività effettivamente svolte e ogni eventuale trattamento correlato che, in ragione della natura e delle peculiarità dell'attività stessa, risultano potenzialmente esposti a rischi rispetto al diritto alla protezione dei dati personali.

Peraltro, già altre norme – tra cui la Legge 190/2012 ("Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione") – richiedono un modello organizzativo che includa un approccio per processi, ai fini di meglio identificare e prevenire i rischi verso cui sono potenzialmente esposte le attività dell'Ente.

In considerazione di quanto sopraindicato, è opportuno che – in occasione dell'applicazione del GDPR – ogni Ente, se non lo ha ancora effettuato, implementi il Sistema organizzativo con l'approccio per processi.

In particolare, riveste particolare importanza l'identificazione e mappatura dei processi in modo unitario, a prescindere dall'istanza contingente che ne motiva la realizzazione (quali l'applicazione di una specifica norma o la risposta ad una puntuale esigenza gestionale).

Infatti, i processi – rappresentando come effettivamente sono svolte le attività dell'Ente – se declinati con un approccio unitario (valido per tutto l'Ente e per tutte le casistiche applicative) e con la stessa metodologia di rilevazione consentono una più semplice individuazione delle responsabilità, dei potenziali rischi cui sono esposti gli obiettivi di ogni processo e del livello di adeguatezza delle misure di sicurezza, di prevenzione e/o di controllo esistenti.

Inoltre, lo stesso "linguaggio" consente per ogni processo - da un lato - la confrontabilità del grado di rilevanza dei diversi rischi, indipendentemente dall'ambito operativo in cui possono manifestarsi e dall'altro, la rilevazione di ogni misura tecnica e organizzativa applicata ai fini della mitigazione dei rischi rilevati, con la conseguente possibilità di razionalizzare le misure di prevenzione.

In conclusione, l'approccio unitario per processi riveste un ruolo cruciale per l'implementazione e l'aggiornamento di un Sistema Organizzativo in grado di realizzare una gestione dei rischi efficace ed efficiente.

4 Indicazioni per il sistema organizzativo per l'applicazione del GDPR

4.1 Governance e impostazione del sistema organizzativo

4.1.1 Governance e profili di responsabilità per l'applicazione del principio di accountability

In riferimento al Sistema di governance dell'Ente e dell'articolazione dei profili di responsabilità, si definiscono i seguenti ambiti di riferimento ai fini dell'applicazione del GDPR, nel rispetto del principio di accountability.

Si distinguono tre ambiti di riferimento:

- Data Protection Officer (DPO)
- Struttura organizzativa
- Soggetto esterno

Le indicazioni per ogni ambito sono dettagliate nei paragrafi successivi.

4.1.2 Approccio per funzioni e approccio per processi

4.1.2.1 Termini

Un processo aziendale è una sequenza di attività tra loro interrelate e finalizzate al conseguimento di un obiettivo comune, svolte all'interno dell'azienda, che creano valore trasformando delle risorse (input del processo) in un prodotto (output del processo) destinato ad un soggetto interno o esterno all'azienda (cliente).

Con il termine *process owner* si intende la figura a cui è affidata la responsabilità dell'intero processo, che presiede in qualità di coordinatore delle varie funzioni coinvolte. Egli deve garantire il corretto funzionamento del processo nel suo complesso, curandone l'efficacia e l'efficienza.

Si tratta di una figura molto importante, essendo anche preposta ad individuare gli obiettivi del processo, gli indicatori di prestazione ed i possibili interventi di miglioramento. Deve essere in grado di relazionarsi efficacemente, poiché ha il compito di regolare il flusso delle risorse e di sovrintendere a tutte le attività convincendo e motivando i soggetti interni ed esterni al processo ed eliminando le controversie che possono affiorare.

Occorre rilevare che, a differenza dei processi, le procedure non elaborano informazioni, ma descrivono le modalità per elaborare tali informazioni.

In sintesi, si potrebbe affermare che una procedura stabilisce "come" un'attività dev'essere svolta, mentre un processo indica "che cosa" dev'essere fatto per raggiungere un risultato o, più propriamente, "chi deve fare che cosa".

4.1.2.2 Approccio organizzativo per funzioni e per processi

Diamo per conosciute le differenze fra un approccio per funzioni e un approccio per processi, ribadendo che quest'ultimo risulta più rispondente ai dettami del GDPR in quando prende in esame il concatenarsi di

azioni all'interno di un sistema organizzativo andando trasversalmente a coprire più unità funzionali anche di strutture diverse.

Anche in riferimento alle caratteristiche sopraesposte, sono sempre più le norme di legge che richiedono per la loro applicazione Compliance Program un approccio per processi.

In questa logica si pone il GDPR e anche la legge 190/2012 ("Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione).

Evidente è che, sia in fase di individuazione di un trattamento, sia nella fase di valutazione dei rischi e infine nella attribuzione dei compiti in termini di Protezione del Dato si debba tenere presente l'intero processo e non singole funzioni all'interno dell'organizzazione.

L'attenzione ad una visione per processi, oggi molto scarsa nelle organizzazioni pubbliche consentirebbe un miglioramento della visione organizzativa e del suo controllo in termini di obiettivi/risultati ed inoltre consentirebbe una semplificazione nella redazione di compliance program, fra cui il GDPR, che appunto si basano non su funzioni ma su processi.

4.2 Data Protection Officer (DPO)

4.2.1 Funzione e ambiti di attività

Il DPO è incaricato di svolgere almeno i seguenti compiti e funzioni:

a) informare e fornire consulenza al titolare del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal regolamento (UE) 2016/679, nonché da altre disposizioni nazionali o dell'Unione relative alla protezione dei dati;

b) sorvegliare l'osservanza del regolamento (UE) 2016/679, di altre disposizioni nazionali o dell'Unione relative alla protezione dei dati nonché delle politiche del titolare del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;

c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del regolamento (UE) 2016/679;

d) cooperare con il Garante per la protezione dei dati personali;

e) fungere da punto di contatto con il Garante per la protezione dei dati personali per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 del regolamento europeo, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

Al DPO sono affidati anche i seguenti compiti:

- definire un piano di azioni per la piena applicazione del regolamento (UE) 2016/679 e della normativa di riferimento per la Giunta regionale, avvalendosi delle competenti strutture delle Direzioni, in relazione ai trattamenti di cui sono responsabili;
- definire un piano di azioni per la piena applicazione del regolamento (UE) 2016/679 e della normativa di riferimento per ciascuno degli Enti e Agenzie regionali, avvalendosi delle competenti strutture di ciascun Ente in relazione ai trattamenti di cui sono responsabili;
- svolgere, in collaborazione con la Direzione Diritti di cittadinanza e di coesione sociale, una funzione di coordinamento nei confronti dei Responsabili della Protezione dei Dati (DPO) del sistema sanitario regionale e delle relative strutture.

4.2.2 Struttura dell'Ufficio DPO

Il DPO riferisce direttamente al titolare del trattamento che ne dispone la collocazione all'interno della struttura dell'ente in osservanza ai principi di suddivisione delle responsabilità.

La struttura dell'Ufficio a supporto del DPO monocratico è composta da più persone – interne all'organizzazione - nel rispetto dei requisiti disposti dal GDPR, con particolare attenzione all'articolazione di competenze multidisciplinari e all'assenza di conflitti di interesse.

4.2.3 Rapporti con le direzioni e i settori dell'Ente

Per ogni Direzione deve essere individuata una persona di riferimento (Referente interno), con adeguate competenze in ambito di applicazione del GDPR, che supporta la propria Direzione competente per tutte le questioni attinenti al trattamento dei dati personali e che rappresenta l'interlocutore operativo presso l'ufficio del DPO.

I Referenti svolgono attività informativa nei confronti dell'Ufficio del DPO, perché quest'ultimo abbia tutti gli elementi e riscontri che – unitamente alle evidenze della documentazione richiesta dal GDPR – i trattamenti di dati personali svolti nell'ambito di ogni Direzione siano effettuati in conformità alle prescrizioni del GDPR e alle istruzioni del Titolare.

In particolare, i Referenti – in riferimento ai trattamenti svolti nella Direzione in cui sono collocati - devono supportare la propria Direzione competente per:

a) la mappatura dei processi
b) il censimento dei trattamenti di dati personali svolti
c) l'individuazione e la valutazione dei rischi cui è potenzialmente esposto ogni trattamento svolto rispetto al diritto alla protezione dei dati personali
d) l'individuazione e la valutazione delle misure di sicurezza adeguate a prevenire i rischi individuati
e) il monitoraggio costante dell'attuazione delle misure di sicurezza
f) l'assolvimento di ogni altro adempimento disposto dal GDPR e dalle Istruzioni del Titolare
g) la predisposizione di ogni contenuto per la formalizzazione degli adempimenti assolti.

4.2.4 Profili dei componenti dell'Ufficio DPO

Il responsabile della protezione dei dati è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39.

Per svolgere adeguatamente la sua funzione, il DPO dovrà avere qualità professionali adeguate alla complessità dei trattamenti di dati posti in essere dall'ente: a tal fine, il DPO dovrà essere selezionato tra figure con competenze tecnico-legali e/o con esperienza in materia di protezione dei dati.

Il Garante per la protezione dei dati personali ha indicato che non è obbligatorio che il DPO possieda attestazioni o certificati. La sussistenza di adeguate competenze deve essere semplicemente documentata, ad esempio con le esperienze pregresse o la partecipazione a corsi professionali o altre soluzioni che possono essere valutate adeguatamente.

Per un adeguato presidio del requisito dell'articolazione delle competenze multidisciplinari i profili dei componenti l'Ufficio del DPO devono collegialmente possedere conoscenze nei seguenti ambiti:

- giuridico, con competenze privacy e data protection
- informazione, comunicazione e formazione
- organizzazione
- gestione trattamenti
- informatiche e sicurezza delle informazioni.

Ulteriori conoscenze ed esperienze pertinenti sono:

- conoscenza della normativa e delle prassi nazionali ed europee in materia di protezione dei dati, compresa un'approfondita conoscenza del GDPR;
- familiarità con le operazioni di trattamento svolte;
- familiarità con tecnologie informatiche e misure di sicurezza dei dati;
- conoscenza dello specifico settore di attività e dell'organizzazione del titolare/del responsabile;
- capacità di promuovere una cultura della protezione dati all'interno dell'organizzazione del titolare/del responsabile.

Non possono essere nominati DPO o componenti dell'Ufficio DPO soggetti che ricoprono ruoli nell'organizzazione che possono determinare potenziali conflitti d'interesse o il mancato rispetto dei principi di controllo, con particolare attenzione al principio della segregazione delle funzioni.

Il DPO e i componenti dell'Ufficio del DPO non possono rivestire ruoli che comportino la definizione di finalità e mezzi di trattamento.

4.2.5 Flussi informativi da e verso il DPO

4.2.5.1 Flussi informativi da parte del DPO

Il DPO segnala al Titolare del trattamento le violazioni accertate che possano comportare l'insorgere di una responsabilità in capo all'Ente per non conformità al GDPR, anche ai fini degli opportuni provvedimenti.

I flussi informativi dal DPO al Titolare del trattamento avvengono su una base continuativa e riguardano ogni aspetto che il DPO ritiene di sottoporre al Titolare, ai fini della conformità al GDPR, tra cui si citano a titolo esemplificativo:

a) informazioni sul livello di adeguatezza della sicurezza e della capacità di prevenzione di trattamenti in violazione del Regolamento
b) evidenze di ipotesi di trattamento a "rischio elevato"
c) istanze da presentare all'Autorità di controllo
d) ispezioni da parte dell'Autorità di controllo
e) criticità inerente la protezione dei dati personali, anche in relazione ad eventuali segnalazioni esterne o interne ricevute dall'Ente

Nei confronti di tutti i soggetti istruiti e autorizzati dal Titolare del trattamento a trattare dati personali l'Ufficio del DPO fornirà informazioni e consulenza sugli obblighi e sulle misure indicate dal GDPR, a seguito di specifica richiesta ricevuta, con le modalità indicate al paragrafo successivo.

4.2.5.2 Flussi informativi verso il DPO

Il Titolare del trattamento e il Responsabile del trattamento si assicurano che il responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.

Il sistema dei flussi informativi è strutturato in base ai seguenti punti principali:

- ogni direttore, dirigente, posizione organizzativa e/o altre eventuali figure di coordinamento sono tenuti a comunicare al DPO – direttamente o per il tramite del Referente Interno della Direzione competente - ogni evento rilevante ai fini dell'applicazione del GDPR
- i responsabili della Struttura organizzativa interna per la sicurezza dei trattamenti con mezzi elettronici e della Struttura organizzativa per la sicurezza dei trattamenti cartacei devono comunicare tempestivamente al DPO le evidenze di ogni attività di controllo e/o di altra natura rilevante ai fini dell'applicazione del GDPR
- i dati di contatto del DPO da pubblicare dovranno ricomprendere le informazioni che possono consentire agli interessati e al Garante di raggiungerlo con facilità: recapito postale, numero telefonico dedicato e/o indirizzo mail dedicato

- le richieste più specifiche che richiedono un parere da parte dell'ufficio del DPO, avvengono per via telematica secondo le indicazioni riportate sul sito dell'organizzazione di riferimento alla sezione Data Protection Officer – Contatti.

4.2.6 Controlli

In relazione al ruolo previsto dal legislatore europeo che configura il DPO come un supervisore indipendente, il compito del DPO nell'ambito delle attività di verifica è quello di vigilare affinché il sistema dei controlli preventivi (l'insieme delle misure di sicurezza tecniche e organizzative e ogni altro presidio di controllo applicato dall'Ente) nel suo complesso sia adeguato a mitigare i rischi riferibili al diritto alla protezione dei dati personali e a mantenere nel tempo la propria efficacia nel mantenere a livello accettabile i rischi di volta in volta rilevati e/o emergenti.

In sostanza, non competono al DPO né i controlli operativi (c.d. di primo livello) né i controlli ispettivi (c.d. di secondo livello) sull'osservanza del regolamento.

I controlli operativi spettano ai dirigenti, o a loro delegati, in riferimento ai trattamenti di dati personali svolti nel settore di cui sono responsabili. Per tali attività di controllo possono avvalersi del supporto del Referente Interno GDPR collocato nell'ambito della Direzione Competente. Il Referente Interno informa il Direttore responsabile della Direzione competente delle evidenze dei controlli svolti.

I controlli ispettivi sono svolti dai responsabili della Struttura organizzativa interna per la sicurezza dei trattamenti con mezzi elettronici e della Struttura organizzativa per la sicurezza dei trattamenti cartacei, o dai loro rispettivi delegati o incaricati, in corrispondenza dei relativi ambiti di competenza.

Le evidenze di tutti i controlli e di ogni altra attività di verifica effettuata rilevante ai fini del GDPR devono essere comunicate al DPO.

In riferimento alle evidenze dei controlli svolte, alle eventuali segnalazioni ricevute, alla verifica di documentazione e/o ad ogni altra informazione acquisita rilevante ai fini del GDPR il DPO può:

- riservarsi di chiedere approfondimenti ai soggetti competenti per i controlli di primo e secondo livello
- intervenire con una pluralità di azioni idonee a favorire l'osservanza delle prescrizioni del GDPR (a titolo esemplificativo, si veda le ipotesi di intervento in ordine al controllo del registro dei trattamenti, così come indicate nelle Indicazioni Operative per il Registro delle attività di trattamento)
- disporre ulteriori controlli – da effettuarsi dall'Ufficio del DPO o da altri soggetti specificatamente designati dal DPO stesso - negli ambiti di competenza assegnati dal legislatore europeo (sorvegliare l'osservanza del regolamento, nonché delle altre disposizioni europee o di diritto interno in materia di protezione dati; sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e attività di controllo)

Nel rispetto di quanto disposto dall'art. 39, secondo paragrafo, del GDPR ("Nell'eseguire i propri compiti, il DPO considera debitamente i rischi inerenti al trattamento…") il DPO può definire un ordine di priorità nelle attività da svolgere in relazione a quelle che hanno come ambiti di riferimento quelli che presentino maggiori rischi in termini di protezione di dati (c.d. Piano attività Risk Based).

Allo scopo di svolgere le proprie funzioni, il DPO può:

a) partecipare agli incontri organizzati tra Direzioni o Settori competenti, valutando quali tra essi rivestano rilevanza per il corretto svolgimento dei propri compiti
b) accedere a tutta la documentazione e a tutte le sedi rilevanti dell'Ente per lo svolgimento dei propri compiti.

4.2.7 Gestione delle risorse e budget

Il DPO – ai sensi dell'art. 38 del GDPR - deve essere dotato delle risorse necessarie per lo svolgimento efficace dei propri compiti, così come indicati all'art. 39 del GDPR, per accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica.

Ciò implica che:

- sia fornito supporto attivo alle funzioni del DPO da parte delle Direzioni e dei Dirigenti
- siano assegnate adeguate risorse (finanziarie, infrastrutture - sede, attrezzature, strumentazione - e personale)
- sia comunicata ufficialmente la nomina del DPO a tutto il personale, in modo da garantire che la sua presenza e le sue funzioni siano note all'interno dell'Ente
- sia garantito l'accesso alla collaborazione da parte delle Direzioni e dei Settori dell'Ente, così da fornire al DPO supporto, informazioni e input essenziali
- sia assicurata la formazione permanente del DPO e dei componenti dell'Ufficio del DPO, in modo che possano curare il loro aggiornamento con riguardo agli sviluppi nel settore della protezione dati.

Nel rispetto delle procedure dell'Ente applicabili, il DPO provvederà a trasmettere la propria richiesta di budget periodico, opportunamente motivata, al Titolare o ad altro organo delegato dal Titolare.

In riferimento al budget assegnato, il DPO svolgerà in autonomia le proprie attività, con il potere di intervenire – impiegando le risorse necessarie – anche per attività non incluse nella richiesta di budget, se ritenute dal DPO stesso con carattere d'urgenza e/o di maggior rilevanza ai fini dell'applicazione del GDPR.

4.3 Struttura interna

4.3.1 Criteri per l'individuazione dei soggetti e del rispettivo profilo di responsabilità

I criteri principali di riferimento sono:

- ruoli, compiti e responsabilità

- necessità di compiere trattamenti di dati personali nell'ambito delle attività svolte direttamente o da propri collaboratori nell'ambito di funzioni di coordinamento di diverso livello, così come individuati dalla seguente documentazione:
- Statuto
- Legge Regionale del 21/05/2008, n. 28 e s.m.i. istitutiva di Sviluppo Toscana S.p.A.,;
- Disposizione n. 37 del 01 Ottobre 2018 "*Aggiornamento provvedimento organizzativo di Sviluppo Toscana S.p.A*." ;
- Ogni altro documento vigente per la formalizzazione e la rappresentazione della struttura organizzativa.

4.3.2 Ruoli e responsabilità

Come motivato in precedenza il GDPR cambia l'approccio al concetto di privacy ed assegna la responsabilità della protezione del dato in maniera diffusa all'organizzazione del Titolare, mappando tale responsabilità in analogia con tutte le altre secondo il convincimento che il dato sia una risorsa con valore economico e sociale attribuito alla responsabilità di tutti coloro che lo trattano, nell'ambito dei loro specifici ruoli all'interno dell'organizzazione.

In riferimento al sistema di governance in essere, l'articolazione dei ruoli è il seguente:

- Titolare del trattamento: Regione Toscana-Giunta Regionale
- Soggetti istruiti e autorizzati: tutti i direttori, dirigenti e altro personale che nell'ambito delle attività svolte direttamente o da propri collaboratori sia coinvolto nel trattamento di dati personali.

I Soggetti istruiti e autorizzati assumono un diverso livello di responsabilità anche ai fini GDPR in riferimento al ruolo e alle responsabilità ricoperti nella struttura organizzativa dell'Ente.

Ai direttori e ai dirigenti cui è attribuita la rappresentanza legale, la responsabilità delle risorse (finanziarie e umane) viene corrispondentemente assegnata anche la responsabilità dei dati personali, in relazione al valore sociale ed economico degli stessi (Considerando 4).

Il Presidente della Giunta Regionale, ai sensi di quanto previsto dall'art. 4, comma 2, della Legge 1/2009 "Testo unico in materia di organizzazione e ordinamento del personale", può delegare alcune attività del Titolare del trattamento nell'ambito di quanto disposto dalla legge sull'organizzazione dell'ente.

Questo semplifica azzerando la burocrazia introdotta dalla privacy che richiedeva nomine particolari e il loro aggiornamento al cambiare delle persone nei diversi ruoli organizzativi.

Il dirigente assume, a seconda del ruolo gerarchico ricoperto nell'ente la responsabilità della protezione del dato coinvolto nelle competenze a lui assegnate.

4.3.3 Modalità di gestione e strumenti organizzativi

Aggiornamento strumenti organizzativi in coordinamento con il periodico processo di analisi dei rischi e di valutazione dell'adeguatezza delle misure di sicurezza.

Ogni variazione va riportata tempestivamente negli strumenti di formalizzazione e rappresentazione organizzativa vigenti (quali organigramma, rappresentazione e mappatura processi, elenco competenze, mansionari).

Fra gli strumenti organizzativi occorre ricordare l'obbligatorietà dell'attività di informazione, comunicazione e formazione interna tesa a diffondere una cultura e una consapevolezza delle azioni dei singoli come contributo essenziale al sistema della protezione dei dati, che rappresenta un bene comune che tutti sono tenuti a tutelare rispetto ad usi non consentiti o ad abusi.

In questo le strutture interne preposte a tali funzioni sono chiamate a dare comunicazione al DPO e al Titolare, della programmazione e relativo consuntivo sugli interventi di informazione, comunicazione e formazione ritenuti congrui al raggiungimento dell'obiettivo.

4.3.4 Struttura organizzativa per la sicurezza dei trattamenti con mezzi elettronici

4.3.4.1 Premessa

Regione Toscana e gli enti ad essa collegati, nella consapevolezza che le informazioni trattate rappresentano un bene strategico per il raggiungimento degli obiettivi aziendali deve definire e predisporre quanto necessario per implementare un Sistema di Gestione per la Sicurezza delle Informazioni (definito anche come Information Security Management System - ISMS) che permetta di assicurare l'accessibilità e la disponibilità dei dati e delle informazioni trattate.

Riferendosi ad un ISMS non per forza si deve fare riferimento ad un sistema di gestione della sicurezza delle informazioni certificato (es. ISO27001) ma in generale si deve pensare ad un insieme di Politiche, Procedure, Istruzioni operative e quant'altro possa governare e organizzare, in modo unitario e sincrono, tutti i processi per la sicurezza delle informazioni.

In tale ottica, all'interno di un potenziale ISMS, è di fondamentale importanza l'organizzazione e tutti i suoi ruoli primari.

Tutte le figure individuate e suggerite dal presente documento contribuiscono pertanto, ognuna per le parti di propria competenza, a rendere possibile l'adeguata gestione e il raggiungimento degli obiettivi previsti da un ISMS.

Regione Toscana e tutti gli enti ad essa collegata provvederanno a definire, in linea alle presenti indicazioni, le figure più idonee (in base alla dimensione dell'organizzazione, ai trattamenti effettuati, ai rischi valutati, alla esternalizzazione di alcuni processi e ai requisiti cogenti) con la finalità di supportare al meglio il proprio sistema di gestione della sicurezza delle informazioni.

A seguire alcuni spunti organizzativi a copertura dei principali processi della sicurezza delle informazioni.

4.3.4.2 Il Comitato per la Sicurezza delle Informazioni

Il Comitato per la Sicurezza delle Informazioni è di norma costituito dalle principali figure organizzative che ruotano attorno al mondo della sicurezza delle informazioni quali il responsabile delle sicurezza (CISO), il Security Manager, i vari Direttori delle principali aree ICT, le principali direzioni di Business, il DPO e comunque qualsiasi figura che sia ritenuta utile al fine di condividere e definire linee strategiche e indirizzi della sicurezza delle informazioni all'interno della organizzazione stessa. Nel caso di Regione Toscana è importante che all'interno di un possibile Comitato siano presenti anche i rappresentanti degli enti collegati quali DPO, CISO, Security Manager, ecc.

Il Comitato per la Sicurezza delle Informazioni, che può essere convocato sia periodicamente sia su specifica richiesta, può in generale operare per:

- promuovere le Politiche per la Sicurezza delle Informazioni;
- definire direttive chiare e supporto metodologico in materia di Sicurezza delle Informazioni;
- assicurare un presidio strategico sulla continuità delle attività previste dal ISMS;
- identificare dei perimetri di responsabilità e competenze specifiche delle funzioni coinvolte nel ISMS;
- effettuare dei riesami periodici del ISMS;
- definire metodologie e processi specifici per la Sicurezza delle Informazioni;
- valutare l'adeguatezza e monitoraggio dell'attuazione dei controlli specifici per la Sicurezza delle Informazioni;
- assicurare il monitoraggio degli incidenti inerenti la Sicurezza delle Informazioni e la gestione degli eventuali Data Breach;
- promuovere iniziative per accrescere la Sicurezza delle Informazioni;
- promuovere iniziative di formazione ed informazione per accrescere la cultura della Sicurezza delle Informazioni.

4.3.4.3 Il Comitato per la Cyber Security

Oltre al Comitato per la Sicurezza può essere importante definire un comitato più tecnico e specialistico volto ad analizzare ed indirizzare soluzioni di sicurezza al fine di ridurre le vulnerabilità tecniche (ma non solo) all'interno dell'organizzazione. Il comitato, definito come "Comitato per la Cyber Security" può essere composto da vari membri con skill tecnici e specialistici nell'ambito della Sicurezza delle informazioni di Regione Toscana ed Enti collegati. Il comitato per la Cyber Security ha la funzione di coordinare l'eccellenza al fine di progettare un sistema di sicurezza più resistente agli attacchi esterni; migliorare la continuità di servizio delle infrastrutture critiche di Regione Toscana e delle filiere strategiche; sviluppare piani di formazione per aumentare la conoscenza e consapevolezza in termini di cyber-security; aumentare la collaborazione sinergica fra Regione Toscana e i suoi Enti collegati.

4.3.4.4 I ruoli di governo nella sicurezza delle informazioni

Di norma tutti gli aspetti riferiti alla sicurezza delle informazioni all'interno di una Organizzazione possono essere presidiati da uno o più responsabili (in un modello anche di responsabilità distribuite) dove la finalità ultima rimane comunque quella di governare i processi della Sicurezza.

In base alla dimensione della organizzazione, alle informazioni trattate, ai rischi intrinseci e alla complessità delle architetture in alcuni casi sarà ragionevole definire anche molteplici ruoli a supporto della sicurezza (rappresentanti, responsabili, manager, ecc) mentre in altri casi invece si opterà per la definizione di modelli organizzativi più snelli e semplici con ruoli più diretti ed operativi (es. solo dei Responsabili o Security Manager).

Qualsiasi sia la scelta dell'Ente per la definizione del proprio modello organizzativo per la sicurezza delle informazioni deve essere assolutamente chiaro che alcuni processi e attività sono comunque da presidiare, fra cui, in modo particolare:

- proporre e gestire le Politiche per la Sicurezza delle Informazioni;
- garantire la definizione degli obiettivi di controllo e del piano di sicurezza;
- proporre e concordare con il comitato della Sicurezza le risorse necessarie per lo sviluppo ed implementazione delle contromisure di sicurezza derivanti dal piano della Sicurezza;
- definire i ruoli e le responsabilità per la sicurezza delle informazioni;
- rendere noto alla struttura organizzativa l'importanza del raggiungimento degli obiettivi per la sicurezza, del rispetto della politica e delle disposizioni legislative, nonché la necessità di un miglioramento continuo;
- fornire risorse sufficienti a sviluppare, implementare, far funzionare il Sistema di Gestione per la Sicurezza delle Informazioni;
- stabilire il livello di rischio accettabile;
- garantire che tutto il personale cui sono assegnate le responsabilità definite nel ISMS abbia la competenza idonea a svolgere i compiti richiesti;
- garantire che tutto il personale competente sia a conoscenza dell'importanza delle proprie attività inerenti la sicurezza delle informazioni e del proprio contributo al raggiungimento degli obiettivi del ISMS;
- coordinare le attività per la realizzazione del piano di sicurezza;
- coordinare le attività di analisi dei rischi;
- coordinare le attività per la definizione del Piano di continuità Operativa
- partecipa alla revisione dei contenuti del ISMS (riesame nel caso di certificazione ISO27001);
- presidiare la pianificazione degli audit interni;
- presidiare gli aspetti tecnico/di controllo del ISMS attraverso il supporto dell'area tecnica.

Tutte le figure chiamate a Governare i processi della Sicurezza sono di norma membri stabili del Comitato per la Sicurezza delle Informazioni

4.3.4.5 Gli specialisti della Sicurezza

Sono figure operative dedicate alla pianificazione e all'implementazione delle soluzioni per la sicurezza delle informazioni riguardanti applicazioni, sistemi e reti. Gli specialisti gestiscono giorno per giorno la sicurezza di applicazioni, reti, sistemi e del software responsabile dei servizi di rete implementano i controlli di sicurezza come definito dalle policy dell'organizzazione, le linee guida e gli standard. Si interfacciano costantemente con il personale addetto alla verifica o all'organizzazione delle infrastrutture per contribuire alla loro sicurezza. Si occupano inoltre della documentazione tecnica relativa alla sicurezza infrastrutturale. Sono riconosciuti come esperti tecnici della sicurezza ICT dai colleghi.

4.3.4.6 Le responsabilità nella conservazione digitale

Nel caso di conservazione sostitutiva della documentazione a norma di legge così come richiamato dal Codice dell'Amministrazione Digitale (d.lgs. n. 82/2005 e ss. mm.), dal D.M. 23.01.2004 e dal D.P.C.M. 03.12.2013 è necessario che gli Enti definiscano un responsabile che si occupi di governare tali processi (profilo indicato esplicitamente nel documento di accreditamento dei soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici). Tale figura professionale definisce e attua le politiche per la sicurezza del sistema di conservazione digitale e ne governa la gestione operando di concerto con i vari responsabili dei trattamenti, con il Responsabili della sicurezza delle informazioni, con il responsabile dei sistemi informativi ed il responsabile della gestione documentale.

È bene che anche tale figura, quando presente, sia membro del Comitato della sicurezza delle informazioni.

4.3.4.7 Le responsabilità nella gestione degli incidenti

È bene che siano definite delle figure a gestione del processo di raccolta, gestione e analisi degli incidenti fra cui anche tutto il processo di Data Breach previsto dal GDPR.

Che sia definito uno specifico manager (Incident Manager) piuttosto che si faccia riferimento a ruoli già esistente quali ad esempio dei Security Manager o in taluni casi direttamente anche al Responsabile della sicurezza delle informazioni è bene che le responsabilità per le seguenti attività sia definite e formalizzate:

- mantenere un registro degli incidenti
- valutare l'impatto sulla continuità del servizio coordinandosi con l'eventuale responsabile della continuità operativa
- supervisionare il gruppo di intervento e gli specialisti nelle attività di contrasto degli incidenti durante le fasi di emergenza
- segnalare al DPO possibili vulnerabilità e/o incidenti in ambito di trattamento di informazioni personali
- analizzare lo storico degli incidenti insieme agli specialisti al fine di identificare delle soluzioni stabili in grado di contrastare le vulnerabilità emerse

- comunicare al CISO (quando presente) la sintesi delle vulnerabilità emerse dal registro degli incidenti e le soluzioni intraprese per il loro contrasto
- procede alla notifica al CSIRT Italiano quando previsto in accordo con il titolare e il DPO
- supportare il Titolare del trattamento (o a suo delegato) e il DPO nel processo di notifica del Data Breach al Garante
- supportare il Titolare del trattamento (o suo delegato) e il DPO nel valutare la necessità di procedere anche alla comunicazione dell'incidente a tutti gli Interessati.

4.3.4.8 Gli Amministratori di Sistema

Anche se il GDPR non entra nella specificità della gestione degli "Amministratori di sistema" (definiti anche ADS) si tenga presente che ad oggi il provvedimento in materia dell'Autorità Garante italiana del 25/11/2008 (e s.m.i. del 25/9/2009) è ancora in vigore.

Tale provvedimento, non in contrasto con gli indirizzi e le prescrizioni del GDPR, prevede alcuni obblighi ben precisi in materia di ADS che rimangono tutt'ora validi fa cui:

- È obbligo per il Titolare designare individualmente i singoli amministratori di sistema, a mezzo di un atto che deve elencare analiticamente gli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.
- I titolari sono tenuti a riportare in un documento interno gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad esse attribuite.
- Nel caso in cui i servizi di amministrazione di sistema siano esternalizzati, l'elenco di cui sopra sia conservato, indifferentemente, dal titolare o dal responsabile esterno del trattamento.
- Il Titolare deve adottare sistemi idonei alla registrazione degli accessi logici da parte degli amministratori ai sistemi di elaborazione e agli archivi elettronici (il log deve essere registrato e conservato per almeno 6 mesi).
- Qualora gli amministratori, nell'espletamento delle proprie mansioni, trattino dati personali dei lavoratori, questi ultimi hanno diritto di conoscere l'identità dei predetti. In tal caso, è fatto onere al Titolare di rendere noto ai lavoratori dipendenti detto loro diritto.
- L'operato degli amministratori di sistema deve essere oggetto di verifica, con cadenza almeno annuale, per acclarare che le attività svolte dall'amministratore siano effettivamente conformi alle mansioni attribuite.

4.3.5 Struttura organizzativa per la sicurezza dei trattamenti cartacei

La struttura organizzativa e i profili di responsabilità inerenti la gestione dei trattamenti su supporti cartacei è regolamentata dalla Disciplina del protocollo e degli archivi.

In particolare, si aggiunge la responsabilità:

- nella individuazione e comunicazione di data Breach (violazione del dato) in collaborazione con il Security manager

- nella stesura di regole comportamentali per i dipendenti tesi a responsabilizzare sulla tenuta di archivi o copie cartacei, stampa documenti e del loro smaltimento;

- nella revisione delle regole di gestione degli archivi correnti, dell'archivio storico ecc. alla luce del GDPR.

4.3.6 Aggiornamento della struttura organizzativa interna e dei correlati profili di responsabilità

In relazione all'aggiornamento dei ruoli e delle responsabilità vanno corrispondentemente aggiornati i profili di responsabilità ai fini GDPR.

4.4 Soggetti esterni

4.4.1 Criteri per creazione del registro del profilo di responsabilità e rischio dei fornitori/servizi ruoli e responsabilità

I criteri principali di riferimento sono:

- necessità di compiere trattamenti di dati personali nell'ambito delle attività svolte direttamente o da propri collaboratori nell'ambito dell'esecuzione dei contratti di fornitura,

così come individuati dalla seguente documentazione:

- contratto disciplinante il rapporto di fornitura e eventuali documenti correlati

4.4.2 Modalità di gestione e strumenti organizzativi

Aggiornamento attività disciplinate nei contratti, in coordinamento con il periodico processo di analisi dei rischi e di valutazione dell'adeguatezza delle misure di sicurezza.

Ogni eventuale aspetto rilevante ai fini dell'applicazione GDPR va riportato nella documentazione del sistema di gestione dei rapporti con i fornitori.

A tale scopo risulta utile suggerire una rilevazione puntuale di tutti i contratti in essere, una loro valutazione in termini di rischi per la Protezione dei Dati e per questi un aggiornamento per la compliance con il GDPR.

4.4.3 Aggiornamento dei profili di responsabilità

In riferimento a modifiche contrattuali e/o a variazioni nel servizio che possano potenzialmente comportare una diversa esposizione al rischio e/o una diminuzione del livello di adeguatezza delle misure di sicurezza, in coordinamento con il periodico processo di analisi dei rischi e di valutazione dell'adeguatezza delle misure di sicurezza.

5 Sistema disciplinare con meccanismi sanzionatori

5.1 Violazioni

Le linee guida che il Titolare dovrà predisporre per l'Organizzazione dell'Ente dovrà prevedere quanto meno l'individuazione della casistica delle possibili violazioni con riguardo ai diversi trattamenti e con

riferimento agli obblighi giuridici del Titolare del trattamento così come delineati dalla normativa in materia di protezione dei dati personali.

Questo anche al fine di agevolare il controllo della compliance e l'adozione delle misure di contenimento del relativo rischio.

Con il termine violazioni si fa riferimento a quelle irregolarità – commesse sia da soggetti interni all'Ente che da fornitori esterni - nella gestione dei trattamenti di dati personali che possono potenzialmente esporre l'Ente a sanzioni o essere oggetto di sanzione a seguito di controllo delle autorità di controllo individuate.

5.2 Sanzioni

A prescindere dalle sanzioni previste dal GDPR, è auspicabile che tutti gli Enti destinatari adottino un Sistema disciplinare, con il massimo livello di coordinamento possibile.

La predisposizione di un efficace sistema disciplinare con meccanismi sanzionatori per la violazione delle disposizioni del GDPR e/o delle prescrizioni delle Linee Guida predisposte dall'Ente per l'applicazione del GDPR, è condizione essenziale per garantire l'effettività delle Linee Guida e del correlato GDPR Compliance Program attuato dall'Ente.

L'applicazione delle sanzioni disciplinari prescinde dall'esito di eventuali procedimenti da parte delle Autorità competenti, in quanto le regole imposte dal GDPR Compliance Program sono assunte dall'Ente in piena autonomia.

In particolare, è opportuno che l'Ente adotti un sistema disciplinare con misure sanzionatorie che:

- sia applicabile a tutti i soggetti coinvolti nell'applicazione del GDPR e del Compliance Program attuato dall'Ente, sia che siano figure interne (di ogni livello della struttura organizzativa) che fornitori esterni
- individui puntualmente le sanzioni disciplinari da adottarsi nei confronti di soggetti che pongano in essere violazioni, infrazioni, elusioni, imperfette o parziali applicazioni delle prescrizioni contenute nel GDPR, nelle Linee Guida e nel GDPR Compliance Program adottati dall'Ente, il tutto nel rispetto delle relative disposizioni dei CCNL e delle prescrizioni legislative applicabili
- preveda un'apposita procedura di irrogazione delle suddette sanzioni, individuando il soggetto preposto alla loro irrogazione e in generale a vigilare sulla osservanza, applicazione ed aggiornamento del sistema disciplinare;
- introduca idonee modalità di pubblicazione e diffusione.

6 Allegati

6.1 Schema di riferimento per gli altri Enti

6.1.1 Premessa

Il presente documento ha l'obiettivo di definire uno schema di riferimento destinato a tutte gli Enti Destinatari per la realizzazione delle proprie Linee Guida per l'Organizzazione per la GDPR Compliance.

Si intende in tal modo favorire la realizzazione di un sistema di controllo preventivo coordinato che coniughi la coerenza con gli elementi comuni a Regione Toscana e a tutti gli altri Enti Destinatari con il rispetto delle caratteristiche proprie di ogni Ente.

6.1.2 Impostazione

Lo schema indica tutti gli elementi di riferimento per la realizzazione delle Linee Guida, evidenziando:

- la struttura tipo;
- le parti comuni per tutti gli Enti;
- le parti personalizzabili in relazione alle specifiche proprie di ogni Ente.

Lo schema è rappresentato con l'indice proposto per la struttura comune, con a fianco di ogni voce la qualifica di parte comune o personalizzabile.

6.1.3 Indice Schema di riferimento

Capitolo	*paragrafo*	*natura parte*
Contesto di riferimento	Contesto di riferimento	comune
Premessa	Oggetto e obiettivo del documento	comune
	Ambito di applicazione del documento	personalizzabile
	Aggiornamento e validità del documento	comune
Quadro Normativo	Definizioni normative di riferimento	comune
	Sistema organizzativo previsto dalla normativa	comune
	Ulteriori riferimenti per il sistema organizzativo	comune
Sistema organizzativo dell'Ente	Inquadramento	personalizzabile
	Componenti	personalizzabile
Indicazioni per il sistema organizzativo per l'applicazione del GDPR	Governance e impostazione del sistema organizzativo	comune
	Data Protection Officer (DPO)	personalizzabile
	Struttura interna	personalizzabile
	Soggetti esterni	personalizzabile
Sistema disciplinare con meccanismi sanzionatori	Violazioni	comune
	Sanzioni	comune