SviluppoToscana S.p.A.

Data Protection Policy

Sviluppo Toscana s.p.a.

Modello Organizzativo

INDICE

Scopo del documento

Il presente documento definisce il modello organizzativo della struttura amministrativa di di Sviluppo Toscana S.p.A. per la compliance con il regolamento europeo 2016/679 denominato GDPR. Nello specifico prende in esame le figure organizzative, i processi, ruoli e le responsabilità previste dal GDPR per perseguire l'obiettivo di garantire un adeguato livello di protezione nella gestione di dati personali, e descrivere come debba mutare l'assetto organizzativo dell'azienda al fine di garantire nel trattamento dei dati personali la tutela dei diritti di libertà delle persone.
Si articola quindi in una breve descrizione di cosa richiede l'attuazione del GDPR, quali processi aggiuntivi debbano essere posti in essere e come questi si rapportino con i procedimenti in essere.
A tale documento di definizione del modello organizzativo seguiranno le linee guida per l'attuazione dei processi GDPR individuati.

1 Obiettivo del documento

Il GDPR riforma il precedente impianto normativo in materia di protezione dei dati personali – Codice Privacy, inserendo come innovativo elemento cardine il principio di Accountability (o "Responsabilizzazione") in capo al Titolare, e ad 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 richiesto dal Regolamento al "tema privacy" da parte del Titolare del trattamento, oggi chiamato a rimodulare i processi di gestione dei dati personali secondo **i principi di Data Protection "by design" e "by default"**, per avere la certezza che le misure tecniche e organizzative siano adottate ed integrate fin dalla progettazione (ideazione) del trattamento; per valutare i rischi di minacce che possono generare violazioni dei dati personali (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 prioritizzare gli interventi, per avere la garanzia della liceità del trattamento, per monitorare costantemente le misure di sicurezza ed i trattamenti, per rendere i collaboratori, nella qualità di soggetti autorizzati, consapevoli del valore del dato attraverso la formazione e la corretta applicazione di istruzioni ad hoc 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'azienda 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 le linee guida su come configurare il nuovo assetto organizzativo in materia di protezione dei dati personali.

1.1 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 "Data Protection compliance" basata su metodologie di valutazione del rischio e che deve essere integrata nei processi dell'azienda.
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.

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 di 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:

a. trattati secondo "liceità, correttezza e trasparenza"
b. raccolti per "finalità determinate, esplicite e legittime"
c. adeguati, pertinenti e limitati rispetto alle finalità
d. esatti
e. limitati nella conservazione
f. 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, autonomamente o in regime di contitolarità.
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 tutte le caratteristiche specifiche che influiscono sul processo di determinazione delle finalità e dei mezzi del trattamento di dati personali.
In conclusione, le specifiche del modello organizzativo amministrativo adottato costituiscono l'elemento qualificante per determinare le scelte della volontà (e le modalità di esercizio delle stesse) attraverso la struttura amministrativa che le compete, incluse quelle relative alle finalità e ai mezzi del trattamento di dati personali.

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, tra l'altro, per gli enti pubblici.
Il DPO è parte dell'organizzazione Data Protection dell'azienda, di cui non necessariamente deve essere un dipendente, ben potendo tale ruolo essere assolto da un soggetto esterno identificato dal Titolare o dal 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.
Il DPO è incaricato, dal Titolare del trattamento, 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.
f. fungere da punto di contatto per gli interessati, per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento.

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.
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 separazione 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, né può ricevere istruzioni dal Titolare sulle modalità di esecuzione dei propri compiti.

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:

a. il Direttore Generale ogni Responsabile di Funzione e/o altre eventuali figure di coordinamento sono tenuti a comunicare al DPO ogni evento rilevante ai fini dell'applicazione del GDPR
b. iil Responsabile interno per la sicurezza dei trattamenti con mezzi elettronici ed ogni Responsabile di Funzione, responsabile della sicurezza dei trattamenti cartacei di propria competenza, devono comunicare tempestivamente al DPO le evidenze di ogni attività di controllo e/o di altra natura rilevante ai fini dell'applicazione del GDPR
c. 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
d. 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.

In relazione al ruolo previsto dal legislatore europeo che configura il DPO come un consulente 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'azienda) 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. Per tale attività si avvale del Security Manager.
In sostanza, non competono al DPO i controlli operativi sull'osservanza del regolamento. Per controlli operativi si intendono quei controlli sull'operato dei dipendenti assegnati alla struttura.
I controlli operativi spettano al Direttore Generale o ai singoli Responsabili di ASA/Funzione sul personale agli stessi assegnati a norma del CCNL aziendale e del contratto di lavoro, in riferimento ai trattamenti di dati personali svolti nel nell'ASA/Funzione di cui sono responsabili. Per tali attività di controllo in merito alla correttezza delle operazioni e non dei comportamenti, possono avvalersi del supporto dei Data Protection Specialist.
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 svolti, alle eventuali segnalazioni ricevute, alla verifica di documentazione e/o ad ogni altra informazione acquisita rilevante ai fini del GDPR, il DPO può:

a. riservarsi di chiedere approfondimenti ai soggetti competenti per i controlli
b. intervenire con una pluralità di azioni idonee a favorire l'osservanza delle prescrizioni del GDPR (a titolo esemplificativo, si vedano 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)
c. disporre ulteriori controlli ai fini del processo di accountability – 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 l Direttore Generale ed i Responsabili di ASA/Funzione, valutando quali tra essi rivestano rilevanza per il corretto svolgimento dei propri compiti. A tal fine, in osservanza al principio di Data Protection by Design, ogni qualvolta siano in trattazione argomenti e attività che comportano trattamento di dati personali, occorre, secondo le regole organizzative dell'azienda, darne comunicazione al DPO, che valuterà se e come intervenire.
b. accedere a tutta la documentazione e a tutte le sedi rilevanti dell'azienda per lo svolgimento dei propri compiti
c. 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.

In riferimento al budget assegnato da parte della Regione Toscana, 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 indispensabili per il rispetto della normativa.

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 anche a obblighi risarcitori per mancanze ad esso ascrivibili e, in caso disattenda le istruzioni del titolare al punto da individuare - con i dati che ha ricevuto in affidamento - proprie finalità del trattamento, diventa a sua volta Titolare autonomo, con conseguente applicazione del quadro di riferimento - anche sanzionatorio - ben più "pesante", rispetto a quello relativo ad una semplice violazione degli obblighi contrattuali assunti con il Titolare.
Il Responsabile del trattamento deve presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate – in primis agli standard stabiliti dal titolare - 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 stipulato con il titolare. Il contratto deve regolare gli elementi essenziali del trattamento di dati personali curato dal Responsabile, con particolare riferimento a:

a. materia disciplinata
b. durata del trattamento/i,
c. natura e finalità del trattamento/i,
d. tipo di dati personali
e. categorie degli interessati coinvolti,
f. nonché a tutti gli altri elementi indicizzati all'art. 28, comma 3, GDPR

definendo in modo chiaro quali siano gli obblighi e i diritti del titolare e quali quelli del responsabile, tendo nel debito conto l'attività di controllo propria del Titolare.

5 Autorizzati

Ai fini di individuare gli "autorizzati", al trattamento dei dati personali, si deve far riferimento alle seguenti disposizioni del GDPR:
1. trattasi innanzitutto di persone soggette alla "autorità diretta del Titolare o del Responsabile" (art. 4, § 10)
2. Che non possono trattare dati personali del titolare per il quale operano se non dietro istruzione fornita dal Titolare o dal Responsabile del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri (artt. 29 e 32 § 4)

Quindi per trattare i dati bisogna essere soggetti istruiti e autorizzati.

6 La compliance al GDPR

Passiamo a definire come le figure previste dal GDPR si mappano con ruoli e responsabilità dell'organizzazione aziendale, per rispondere al dettato regolamentare europeo. Lo faremo facendo un breve riepilogo delle figure previste dal GDPR.

7 Le figure e le responsabilità nell'organizzazione

Il Regolamento europeo 2016/679 (GDPR) richiede che le organizzazioni adottino una struttura (ruoli e funzioni) e procedimenti che garantiscano intrinsecamente, così come previsto all'art. 1

(C1-14, C170, C172), la protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché la libera circolazione di tali dati, proteggendo i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali.
Questo in quanto le finalità sono la protezione per l'affermazione di diritti delle persone fisiche, commisurata alla riduzione dei rischi derivanti dall'uso improprio o illecito di dati personali.
A tale scopo il GDPR introduce figure organizzative, con ruoli e responsabilità precisi, e fissa alcuni principi organizzativi atti a vincolare i comportamenti in modo che siano coerenti con le finalità del regolamento stesso.

8 Figure previste esplicitamente o implicitamente dal regolamento

Titolare del Trattamento dati, art. 24 GDPR (C74-C78) (in inglese Controller) è colui che ha la responsabilità, fra le altre, di mettere in atto misure tecniche ed organizzative *adeguate* per garantire, ed essere *in grado di dimostrare* (principio della accountability), che il trattamento è effettuato in modo conforme al regolamento. A lui è demandata in via diretta o indiretta la tutela dei diritti e delle libertà fondamentali della persona fisica a cui si riferiscono i dati personali che vengono trattati. Decide in ordine a finalità e mezzi (questi ultimi parzialmente delegabili a responsabili) dei trattamenti di propria competenza e ha la responsabilità di tenuta del registro dei trattamenti ex art. 30 GDPR (C82).

Delegato del trattamento *ex* ***art.*** .2-quaterdecies, comma 1, D.Lgs. n. 196/2003 è la persona fisica delegata, con atto espresso dal Titolare o dal Responsabile del trattamento, a svolgere le sue funzioni a norma del GDPR sotto la sua responsabilità e nell'ambito del proprio assetto organizzativo.

Responsabile del Trattamento, Art. 28 GDPR (C81) (in inglese Processor) Persona fisica o giuridica, diversa dal Titolare ed esterna all'organizzazione dello stesso, che eventualmente effettua trattamenti per conto del Titolare. Il rapporto fra Titolare e Responsabile, ove previsto, deve essere regolato da apposito contratto o altro atto bilaterale. Al Titolare spetta l'onere e la responsabilità di indicare al responsabile le modalità di trattamento e le relative istruzioni, nonché di controllare che siano rispettate.

Gli autorizzati, ***a***rt .2-quaterdecies, comma 2, d.lgs. 196/2003 sono le persone autorizzate dal titolare al trattamento dei dati: al Titolare compete di dare, oltre che l'autorizzazione, anche le istruzioni e un'adeguata formazione in merito alle misure da adottare nella esecuzione del trattamento.

Data Protection Specialist, figura implicitamente prevista dal GDPR, quando prevede e mette in capo al titolare, responsabilità e attività che prefigurano competenze tecniche specialistiche, non riconducibili direttamente alle competenze richieste per svolgere il ruolo di Titolare. In particolare la valutazione dei rischi (DPIA Art. 35 C84, C89-C93, C95), l'individuazione dei trattamenti partendo dai processi dell'organizzazione e andandone ad individuare i riferimenti che ne determinano la liceità, la determinazione della misura dei rischi di natura tecnica ed organizzativa, ecc. Una figura che abbia competenze organizzative, giuridiche e tecnologiche, o coadiuvata da altre, per essere in grado di supportare la la Direzione nei rapporti con strutture specialistiche, interne o esterne all'all'azienda, referenti per le specifiche competenze.

Security manager/Data Security Officer, figura implicitamente prevista dal GDPR, per garantire quanto previsto alla sezione 2 "sicurezza dei dati personali" , per supportare il Titolare nei suoi compiti di supervisione e controllo delle misure di sicurezza adottate, per determinarne la loro

adeguatezza nel tempo e per garantire il rispetto del principio di separazione delle responsabilità fra chi le misure le deve attuare, il *Responsabile della sicurezza IT* dell'organizzazione o il *Responsabile del trattamento*, e chi invece deve controllarle.

Il DPO (Data Protection Officer), o Responsabile della protezione dei dati, previsto sezione 4 del GDPR art. 37-39. Svolge azione di promozione, consulenza e verifica per il corretto comportamento organizzativo in ottemperanza al regolamento. Mantiene relazioni con l'autorità garante e funge da punto di contatto con gli interessati per agevolare l'esercizio dei loro diritti.

L'ufficio del DPO, struttura non esplicitamente prevista nel GDPR ma derivante dall'esigenza: di essere un punto di competenza multidisciplinare a supporto del Titolare e suoi delegati, di essere punto di contatto con gli interessati, di essere punto di riferimento organizzativo di supporto alle interlocuzioni con il Garante.

9 Come si mappa l'organizzazione GDPR con l'organizzazione dell'azienda:

L'**Amministratore Unico**, in qualità di Direttore Generale assume a norma dell'art. 4, punti 7 e 8, del GDPR,:

- il ruolo di "*Titolare dei trattamenti"* afferenti alle attività c.d. di "funzionamento aziendale" quali la gestione del personale, degli acquisti, degli incarichi professionali, della gestione dei conti correnti, etc.;
- il ruolo di "*Responsabile dei trattamenti*" per i trattamenti afferenti alle attività "istituzionali" di cui all'art. 2 della L.R. n. 28/2008, ai sensi della Convenzione Quadro approvata con Delibera di Giunta e sottoscritta con la Regione Toscana.

Avvalendosi della facoltà prevista dall'art. 37, paragrafo 3, del GDPR, che consente di procedere alla nomina condivisa di uno stesso DPO, in considerazione delle dimensioni delle relative strutture organizzative, dell'affinità tra la tipologia di funzioni, attività e trattamenti di dati personali, oltre che a fini di omogeneità nell'indirizzo e nell'applicazione della relativa disciplina e di razionalizzazione della spesa, Sviluppo Toscana S.p.A. ha individuato come DPO il Dirigente Regionale nominato Data Protectin Officer dalla Regione Toscana con Decreto del Segretario Generale n. 72/2018 (Disposizione dell'Amministratore Unico di Sviluppo Toscana S.p.A. n. 15 del 04/05/2018).

I singoli Responsabili di ASA/Fnzione possono assumere il ruolo didi *Delegati del Titolare e Delegati del Responsabile*

Un responsabile informatico è stato nominato *Security Manager /Data Security Officer.*

I dipendenti, alle dirette dipendenze dell'Amministratore Unico, ai quali, a seguito di un processo autorizzativo da parte del Titolare/Responsabile che integra l'autorizzazione generale e le istruzioni di cui alla Disposizione n. 40/2018, sono associati, nel caso di procedure IT, i diritti di accesso ed elaborazione dei dati o assegnate funzioni per il trattamento di dati personali presenti in documenti o archivi cartacei, vengono associati ai trattamenti tramite registrazione nel Registro dei Trattamenti e assumono il ruolo di *Autorizzati al trattamento.* In tale fase il Titolare/Responsabile, può fornire se lo ritiene utile, ulteriori informazioni e istruzioni utili al dipendente, al fine di consentirgli di svolgere il suo ruolo nella piena consapevolezza del suo operato. Tali **dipendenti,** opportunamente formati, assumono e assolvono alla funzione di *Data Protection Specialist.*

10 I Processi GDPR

La compliance al GDPR si sostanzia nella messa in atto di un modello organizzativo che si innervi nella realtà organizzativa dell'azienda e di processi specifici finalizzati alla costante verifica dei dati trattati e della adeguatezza delle misure adottate e commisurate alla valutazione dei rischi. Altro aspetto che la compliance deve garantire è l'esercizio dei diritti degli interessati.

10.1 Processo: Data protection by design e by default

Questo processo riguarda il rispetto di quanto disposto art. 25 del GDPR, ed è rappresentato da tutte quelle analisi e valutazioni da effettuare al momento della emissione di un qualsivoglia atto che comporti come conseguenza un trattamento di dati personali. Nel caso in cui l'atto prefiguri il trattamento di dati personali devono essere valutati, al livello di granularità commisurato alla tipologia di atto, i seguenti aspetti:

a. Individuazione del trattamento sotteso e del processo organizzativo che si va a ipotizzare o realizzare, modificare, integrare,
b. I soggetti organizzativi coinvolti e le differenti figure dell'organizzazione GDPR,
c. Le relative misure di sicurezza.

Tale processo deve essere vincolante nella produzione di un qualsivoglia atto.
Pertanto si procede alla modifica della procedura dell'iter di approvazione degli atti al fine di inserire una fase di verifica degli impatti GDPR dell'atto, così che se l'atto prefigura il trattamento dei dati personali, l'atto deve essere obbligatoriamente corredato di informazioni aggiuntive ai sensi della disciplina in materia di protezione dei dati personali.
Tale processo è descritto nel documento "*Linee guida per la Data Protection by design e by default*" approvate nel corpo della Data Protection Policy di regione Toscana con D.D. n. 7677/2019 e recepite da Sviluppo Toscana S.p.A. con Disposizione n. 69 del 04/12/2019 nelle parti compatibili con le attività societarie.

10.1.1 Processo: Mantenimento del registro dei trattamenti

L'art. 30 del GDPR (C82) pone in capo al Titolare ed al Responsabile la responsabilità di tenere un registro delle attività di trattamento: pertanto nell'organizzazione aziendale tale responsabilità può essere trasferita trasferisce per delega ai Responsabili di ASA/Funzione nell'ambito dell'esercizio delle loro competenze e dei rispettivi ruoli gerarchici, per effetto di specifico provvedimento organizzativo. Per effetto della Delibera di Giunta Regionale n. 585/2018 è attributo all'ufficio del DPO la supervisione complessiva del registro dei trattamenti per interventi valutativi everifica di qualità sull'operato delle singole strutture e per offrire consulenza, con la dovuta attenzione a non creare conflitto d'interessi, nel senso che il DPO non può essere coinvolto in competenze che prevedono trattamenti di dati personali.
Il registro dei trattamenti viene gestito con apposita procedura IT che deve garantire:

1. il ciclo di vita del trattamento,
2. il collegamento con l'organizzazione dell'ente al fine di mantenere allineate le strutture, le competenze e le persone a seguito di variazioni organizzative, quali cambio di Responsabili, modifiche di competenze delle Aree Strategiche di Attività, cambio di personale autorizzato, etc..
3. il collegamento con i processi produttivi dell'ente in quanto i trattamenti sono segmenti di tali processi finalizzati al trattamento di dati personali. Il riferimento al processo risulta importante in quanto è sulla base del processo, e non del singolo trattamento, che risulta opportuno fare la valutazione dei rischi e la esecuzione di vere e proprie DPIA. Analizzando i singoli trattamenti, può accadere di sottovalutare o sopravvalutare rischi, o di dover eseguire più DPIA, una per

ogni trattamento, con dispendio di costi e tempi, quando sarebbe stato possibile farla una sola volta sull'intero processo (in senso conforme, art 35 comma 1): "… Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi").

4. Il collegamento con gli asset, intesi come applicazioni IT, basi di dati e strutture tecnologiche di supporto, ma anche archivi cartacei e relativi supporti, al fine di determinare le misure di sicurezza
5. Il collegamento con le procedure di assegnazione dei diritti di accesso a dati e funzioni al fine di riportare sui trattamenti correlati, i nominativi degli autorizzati e i relativi privilegi nel trattamento. La gestione degli autorizzati su procedimenti non digitalizzati richiederà l'inserimento manuale degli autorizzati.

Questo prefigura un aggiornamento della procedura IT di gestione dei trattamenti in una logica di processo garante della rappresentazione fedele della realtà.
La gestione dei trattamenti e la loro registrazione nei fatti si configura come un sotto-processo del processo di Data Protection by Design.
Per la descrizione di dettaglio si rimanda alle "*linee guida per il mantenimento del registro dei trattamenti*" (Appendice G delle "*linee guida per la data protection by design e by default*").

10.1.2 Processo: Formulazione e gestione della DPIA

Il GDPR all'art. 35, in coerenza con il principio di sostanziale responsabilizzazione, basato sull'analisi dei rischi, prevede lo strumento della DPIA quale processo mirato alla valutazione degli impatti conseguenti ai rischi rilevati e alla determinazione delle misure finalizzate alla loro riduzione.
La DPIA viene individuata come processo obbligatorio in tutti quei casi in cui, in particolare con l'uso delle di nuove tecnologie, si può presentare un rischio elevato per i diritti e le libertà delle persone fisiche.
Il Garante Nazionale con provvedimento n. 467 del 11 Ottobre 2018 (Pubblicato sulla Gazzetta Ufficiale n. 269 del 19 novembre 2018) ha individuato, così come previsto all'art. 35 comma 4 del GDPR, le tipologie di trattamenti per i quali la DPIA è un adempimento obbligatorio:

a. Trattamenti valutativi o di scoring su larga scala, nonché trattamenti che comportano la profilazione degli interessati nonché lo svolgimento di attività predittive effettuate anche on-line o attraverso App, relativi ad "aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato.
b. Trattamenti automatizzati finalizzati ad assumere decisioni che producono "effetti giuridici" oppure che incidono "in modo analogo significativamente" sull'interessato, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto in essere (ad es. screening dei clienti di una banca attraverso l'utilizzo di dati registrati in una centrale rischi).
c. Trattamenti che prevedono un utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti, effettuati anche on-line o attraverso app, nonché il trattamento di identificativi univoci in grado di identificare gli utenti di servizi della società dell'informazione inclusi servizi web, tv interattiva, ecc. rispetto alle abitudini d'uso e ai dati di visione per periodi prolungati. Rientrano in tale previsione anche i trattamenti di metadati ad es. in ambito telecomunicazioni, banche, ecc. effettuati non soltanto per profilazione, ma più in generale per ragioni organizzative, di previsioni di budget, di upgrade tecnologico, miglioramento reti, offerta di servizi antifrode, antispam, sicurezza etc.
d. Trattamenti su larga scala di dati aventi carattere estremamente personale (v. WP 248, rev. 01): si fa riferimento, fra gli altri, ai dati connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza), o che incidono sull'esercizio di un diritto fondamentale (quali i dati sull'ubicazione, la cui raccolta mette in gioco la libertà di circolazione) oppure la cui violazione comporta un grave impatto sulla vita

quotidiana dell'interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti).

e. Trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti (si veda quanto stabilito dal WP 248, rev. 01, in relazione ai criteri nn.3,7 e8).
f. Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo).
g. Trattamenti effettuati attraverso l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es. IoT; sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi wearable; tracciamenti di prossimità come ad es. il wi-fi tracking) ogni qualvolta ricorra anche almeno un altro dei criteri individuati nel WP 248, rev. 01.
h. Trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche
i. Trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento (es. mobile payment).
j. Trattamenti di categorie particolari di dati ai sensi dell'art. 9 oppure di dati relativi a condanne penali e a reati di cui all'art. 10 interconnessi con altri dati personali raccolti per finalità diverse.
k. Trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento
l. Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.
m.

La decisione o meno di effettuare una DPIA e il suo svolgimento è in capo al titolare o suo delegato che si consulta con il DPO.
I contenuti minimi di una valutazione di impatto sono descritti all'art. 35 comma 7 del GDPR a cui si rimanda.
Il Titolare nello svolgimento della DPIA, se del caso, così come previsto all'art. 35 comma 9 richiede il parere degli interessati o dei loro rappresentanti.
In sintesi il processo di DPIA è competenza del Titolare o suo delegato, che si avvale della consultazione con il DPO ed è mirato ad evidenziare e documentare in modo chiaro i rischi, le misure di sicurezza adottate per mitigarli e i rischi residui. La DPIA è mantenuta aggiornata dal Titolare allorquando si modifichi il processo, intervengano incidenti che mettano in luce possibili debolezze del sistema non considerate, si evidenzino minacce non prese in considerazione, ecc..
La formulazione della DPIA si configura come un sotto-processo del processo di Data Protection by Design da mettere in atto qualora la tematica in questione la richieda.

10.2 Processo: Gestione degli incidenti

È bene che siano definite delle figure per il presidio del processo di raccolta, gestione e analisi degli incidenti fra cui anche il processo di Data Breach previsto dal GDPR.
Che sia definito uno specifico manager (Incident Manager) ove possibile oppure che si faccia riferimento a ruoli già esistenti quali ad esempio dei Security Manager o in taluni casi direttamente anche al Responsabile della sicurezza IT ed è bene che le responsabilità per le seguenti attività siano definite e formalizzate:

a. mantenere un registro degli incidenti
b. valutare l'impatto sulla continuità del servizio coordinandosi con l'eventuale responsabile della continuità operativa
c. supervisionare il gruppo di intervento e gli specialisti nelle attività di contrasto degli incidenti durante le fasi di emergenza

d. segnalare al DPO possibili vulnerabilità e/o incidenti in ambito di trattamento di informazioni personali
e. analizzare lo storico degli incidenti insieme agli specialisti al fine di identificare delle soluzioni stabili in grado di contrastare le vulnerabilità emerse
f. comunicare al Responsabile della sicurezza (quando presente) o al responsabile dello sviluppo dei sistemi informativi o delle infrastrutture (se presente), la sintesi delle vulnerabilità emerse dal registro degli incidenti e le soluzioni intraprese per il loro contrasto;
g. supportare il Titolare del trattamento (o a suo delegato) e il DPO nel processo di notifica del Data Breach al Garante e alle altre autorità competenti.
h. 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.

10.3 Processo: Accountability

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'azienda.
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'azienda 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'azienda.
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, condizione basilare per l'impostazione e la conduzione delle attività di monitoraggio e di accountability.
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.
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:

a. Risk Assessment (identificazione e valutazione dei rischi)
b. 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:

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

Il principio di accountability sancito dal regolamento europeo in materia di protezione dei dati richiede che l'organizzazione e i processi, siano impostati in modo tale a rendere possibile la attività di "rendere conto" delle misure messe in atto per la protezione dei dati.
Principio che si lega fortemente con l'altro della data protection by design in quanto se nella progettazione di nuove iniziative si tiene presente la tematica della protezione dei dati fin dall'inizio e aggiornata nel tempo, l'attività di rendicontazione delle scelte diviene una logica conseguenza della lettura delle decisioni prese e delle relative motivazioni. Se così non fosse e si dovesse rendere conto di quanto fatto solo a valle della rilevazione degli incidenti, ovviamente richiederebbe una ricerca a ritroso non certo agevole sia nel risultato sia nei tempi mettendo il Titolare e tutta l'organizzazione in situazioni sanzionabili a norma del GDPR.
L'organizzazione dell'ente può essere chiamata a rendere conto in varie circostanze:

a. su istanza del Garante in attività ispettiva o a seguito di segnalazioni o denunce
b. su istanza degli interessati nell'esercizio dei loro diritti
c. su istanza del DPO in attività di monitoraggio o a seguito di segnalazioni da parte degli interessati.

In particolare l'attività di "rendere conto" si sostanzia:

a. individuazione del processo in esame
b. rispetto dei principi generali applicabili ai trattamenti,

c. Misure di sicurezza messe in atto sulla base del processo di assessment e di valutazione degli effetti (danni) sulle libertà e i diritti individuali delle persone fisiche, dei rischi, delle minacce e della probabilità di accadimento.

All'interno del Processo di Data Protection by design and by default, è prevista la costituzione di un dossier data protection per ogni processo che tiene traccia delle scelte, delle misure e delle motivazioni che hanno portato alla loro determinazione. Il dossier è tenuto aggiornato come risorsa condivisa dalle diverse figure responsabili dei vari ambiti.
Questo sia che sia stata effettuata a norma dell'art. 35 (C84,C89-C93, C95) una specifica DPIA, sia che non sia stata effettuata in quanto ritenuta non necessaria.

10.3 Processo: Garanzia e tutela dei diritti degli interessati

Il GDPR dedica l'intero Capo III ai diritti dell'interessato ed in particolare:

a. art. 12 trasparenza e modalità attraverso le quali l'interessato viene emesso a conoscenza di come può esercitare i suoi diritti;
b. art. 13 e 14 e informazioni che devono essere fornite all'interessato e le relative modalità;
c. art. 15 i diritti di accesso dell'interessato alla conoscenza di quali dati che a lui si riferiscono sono in possesso del titolare, i relativi trattamenti e quanto a questi è correlato in termini di misure di sicurezza;
d. art. 16 il diritto di rettifica;
e. art. 17 il diritto alla cancellazione (oblio);
f. art.18 il diritto di limitazione del trattamento;
g. art.19 obbligo di notifica da parte del Titolare all'interessato in caso di rettifica, cancellazione, limitazioni;
h. art. 20 Portabilità dei dati, la possibilità cioè, di richiedere e ottenere su adeguato supporto tecnologico e in formati elaborabili i dati detenuti dal Titolare;
i. art. 21 opposizione al proseguimento di un trattamento;
j. art. 22 l'interessato ha il diritto di non essere sottoposto ad un processo automatizzato che produca effetti giuridici che lo riguardano o che incida sulla sua persona, salvo i casi previsti al comma 2 dello stesso articolo.

I diritti richiamati, a norma dell'art. 23 (C73) e per le motivazioni espresse nello stesso articolo, possono subire delle limitazioni.
In estrema sintesi il processo prevede l'informazione preventiva dell'interessato, la richiesta del consenso dove applicabile, come misure antecedenti l'avvio del trattamento con riguardo ad una persona fisica e il diritto della stessa di poter intervenire, con modalità certe e tempi definiti, nell'ambito dei trattamenti e relativi dati che lo riguardano, sia per acquisirne la conoscenza sia per richiedere eventuali misure fra quelle previste dal regolamento.

11 Modello organizzativo da adottare

Come evidenziato, nell'organizzazione Data Protection esistono alcuni ruoli e funzioni chiaramente identificati in capo a determinate istanze organizzative, così come sono chiaramente identificati i processi che sostengono la compliance organizzativa al GDPR.
Ferme restanti le competenze e i vincoli dei diversi soggetti nei rispettivi ruoli, vengono individuate, compatibilmente con la struttura aziendale, le nuove *strutture di supporto e la loro collocazione organizzativa* per il supporto nella gestione dei processi.
Le competenze e le figure di supporto sono quelle riconducibili ai Data Protection Specialist e quelle dei referenti dell'ufficio del DPO.
Nel seguito si prendono i processi GDPR e per ciascuno di essi si descrivono i compiti nei diversi livelli organizzativi.

11.1 Data Protection by design and by default

Tale processo riguarda la "formazione degli atti" (disposizioni e determine) da cui discendono trattamenti di dati personali e la realizzazione di sistemi automatizzati o meno che attuano indirizzi e scelte definiti in tali atti.
Al fine di presidiare il processo di formazione degli atti in modo che sia compliant con il GDPR, nell'azienda possono essere individuate una o più figure di Data Protection Specialist con il compito di supportare il Direttore Generale nel definire, per ogni atto di sua competenza, se è coinvolta o meno la problematica della protezione di dati personali, e se nel caso aggiornare l'atto con quanto necessario ad impostare gli elementi di data protection e seguire l'evoluzione susseguente l'adozione dell'atto stesso. Tale personale costituisce l'interfaccia organizzativa e naturale con il DPO e con l'ufficio del DPO.
Motivazione
Disporre di personale che opera direttamente all'interno dell'azienda, che conosce sia le persone che le problematiche, consente la riduzione dei tempi di valutazione degli atti, il collegare la tematica della protezione dei dati a quella dell'anticorruzione e della trasparenza, fornire un supporto più specifico e contestualizzato in modo omogeno su tutta la direzione. Affiancare il Direttore Generale nei suoi compiti di messa in atto di misure organizzative tese a garantire procedure compliant con il GDPR.
Gli atti, potranno essere centralmente verificati dall'ufficio del DPO che provvederà a formalizzare rilievi e procederà a fare attività di monitoraggio. Per quanto attiene le richieste di pareri verso il DPO nelle diverse fasi di formazione degli atti, che nascono nell'azienda possono avvalersi, dei *Data Protection Specialist* per il supporto diretto e di interlocuzione verso il DPO.

11.1.1 Mantenimento del registro dei trattamenti

Il censimento dei trattamenti per i quali Sviluppo Toscana S.p.A. riveste il ruolo di "Titolare" ed il conseguente aggiornamento del registroè competenza del Direttore Generale o del singolo Responsabile di ASA/Funzione, se ed in quanto delegato dal Titolare. Per i trattamenti per i quali Sviluppo Toscana S.p.A. riveste il ruolo di "Responsabile" nominato dalla Regione Toscana, il censimento e l'aggiornamento dei trattamenti è di competenza del singolo Dirigente, in quanto Delegato del Titolare. In qualità di Responsabile del trattamento, Sviluppo Toscana S.p.A. implementa nel Registro le informazioni prescritte dal comma 2 dell'art. 30 del GDPR.
Le figure di Data Protection Specialist già presenti per supportare il processo di DPbyDD svolgono anche i compiti di supporto ai Responsabili di ASA/Funzione come naturale conseguenza del processo di DPbyDD, nel definire i nuovi trattamenti o la modifica di trattamenti esistenti e supportare, eventualmente, gli estensori nella compilazione del registro.
Motivazione
Tale impostazione consente di disporre:

a) di personale che opera direttamente all'interno della direzione, che conosce sia le persone sia le problematiche, che conosce gli atti che danno luogo a nuovi trattamenti o loro modifiche,
b) di un controllo interno ed omogeneo alla direzione sui processi e sui trattamenti in carico.

11.1.2 Valutazione Impatto (DPIA)

La valutazione di impatto rappresenta una componente fondamentale del processo di data protection by design e by default e costituisce un documento aggiuntivo che va ad aggiungersi alla formazione corretta di atti che per natura dei loro contenuti riguardano trattamenti di "dati particolari".

Il DPO assicura, a norma dell'art. 35 punto 2 e art. 39 lettera c) del GDPR, supporto di consulenza alla redazione delle DPIA. La formulazione della DPIA è competenza del Direttore Generale che emette l'atto.
Pertanto i Data Protection Specialist con il supporto dell'ufficio del DPO o di assistenza esterna (contratti di servizio, convenzioni con università, etc.), hanno il compito di coadiuvare il Direttore Generale nella esecuzione della DPIA.
Motivazione
Le competenze e le conoscenze idonee allo svolgimento di una corretta DPIA sono collocate all'interno dell'azienda.
Per quanto attiene la DPIA questa prevede, nell'attuale sistema messo a disposizione sul sito del Garante, ben 4 figure, l'estensore, il verificatore, il validatore e il DPO cui spetta il compito di formulare il proprio parere.

11.2 Accountability

Premesso che:

a) l'attività di accountability a norma del Regolamento è in carico al Titolare o suo delegato,, che per questo compito si avvale di strutture quali il Security Manager e l'ufficio del DPO;
b) l'attività di monitoraggio tecnico è in carico al Security Manager e all'ufficio del DPO per le valutazioni del caso, e coinvolge per i suoi effetti la struttura interna o la struttura del Responsabile.

In tale contesto il ruolo dell'azienda è quello di offrire il massimo supporto, in maniera diretta o attraverso i Data Protection Specialist, all'ufficio del DPO e al DPO stesso in tutte quelle fasi in cui possa venir richiesto dal Garante o dagli interessati, informazioni in merito ai processi messi in atto al fine di garantire il pieno rispetto del GDPR.

11.3 Monitoraggio, controllo misure di sicurezza e gestione degli incidenti

Tale processo è gestito centralmente dalle strutture del Security Manager, con il supporto dall'ufficio interno del DPO.

11.4 Informazione e Garanzia dei diritti degli interessati

L'informazione agli interessati non può che essere a carico dell'azienda con il supporto consulenziale dell'ufficio del DPO, cui spetta il compito di definire la modulistica

11.5 I compiti dei Data Protection Specialist

Sulla base di quanto sopra espresso si riepilogano i compiti dei Data Protection Specialist.
I DP Specialist 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 dell' siano effettuati in conformità alle prescrizioni del GDPR e alle istruzioni del Titolare.
In particolare, e in riferimento ai trattamenti svolti nell'azienda, supportano, in collaborazione con il Security Manager e l'ufficio del DPO, l'azienda per i seguenti compiti:
a. l'aggiornamento della mappa dei processi,
b. il supporto al Direttore Generale al momento della formazione degli atti al fine di garantire il principio di data protection by design (Determine, Disposizioni, Avvisi pubblici, contratti, convenzioni,… etc.);

c. il supporto al Direttore Generalee ai Responsabili di ASA/Funzione nella individuazione e registrazione corretta dei trattamenti;
d. il supporto al Direttore Generale e ai Responsabili di ASA/Funzione, sulla base delle indicazioni dell'ufficio DPO, in merito alle informative da dare agli interessati;
e. il supporto in accordo con l'ufficio del DPO alla individuazione e la valutazione dei rischi in fase preventiva e di DPIA;
f. richiedere l'intervento del Security Manager per individuare e valutare l'adeguatezza delle misure di sicurezza, sia in fase preventiva sia successiva ad attività di monitoraggio;
g. garantisce il rapporto unitario della direzione nei confronti del DPO per richiesta di pareri e per supporto nel rispondere alle richieste di cittadini;
h. al fineD.Lgs. n. 196/2003, verifica che il personale sia informato e formato sui temi del GDPR e che gli autorizzati abbiano ricevuto e compreso le istruzioni;
i. la piena e fattiva collaborazione all'ufficio del DPO e al Security manager in caso di incidente/data breach e per tutte le azioni conseguenti;
j. la piena e fattiva collaborazione all'ufficio del DPO e al Security Manager in caso di ispezione o indagine delle autorità di controllo.

12 Rapporti fra DPO e il Titolare

Il DPO, nel caso rilevasse criticità di ordine generale in merito all'obiettivo di garantire la compliance al GDPR si attiva direttamente con i referenti interni all'azienda per la risoluzione dei problemi e, ove, qualora questo non portasse a soluzioni entro tempi stimati ragionevoli, provvede a segnalare al Direttore Generale ed al Responsabile IT le criticità organizzative e tecniche o le eventuali violazioni accertate, che possano comportare l'insorgere di una responsabilità in capo all'azienda per non conformità al GDPR-
Tali comunicazioni, su una base periodica e di necessità, riguardano ogni aspetto che il DPO ritiene di sottoporre al Direttore Generale, in qualità di 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.

13 Rapporto fra processi GDPR e Procedimenti decisionali

Nella precedente sezione abbiamo esaminato i processi che il GDPR prevede nell'ambito di una organizzazione compliant, coerente ai suoi principi e ai suoi dettati. In questa sezione delle linee guida, individueremo le misure necessarie a rendere tali processi intrinsecamente connessi con i procedimenti aziendali al fine di non creare percorsi paralleli di difficile gestione e possibili disallineamenti fra i processi decisionali e attuativi e quelli di valutazione dei rischi in caso di trattamenti di dati personali.

13.1 Data Protection by design and by default

Come richiesto dal processo di Data Protection by Design, il tema della protezione dei dati personali deve essere preso in considerazione fin dal nascere di una nuova iniziativa.
Pertanto in ogni atto dell'azienda sia esso una Determina, una Disposizione o altro atto, occorre che sia data evidenza se negli effetti dell'atto vengono coinvolti processi e trattamenti relativi a dati

personali. In questo caso i Data Protection Specialist dell'azienda, con l'ausilio della consulenza dell'ufficio del DPO, provvede ad aprire il "Dossier Data Protection", curandone la tenuta attraverso un aggiornamento costante.
Al fine di dare supporto a tale procedimento occorre:
- che sia adeguata la procedura di gestione degli atti in modo da prevedere una previa verifica circa l'eventuale rilevanza che l'atto specifico possa avere in materia di dati personali, e se sia possibile tradurre alcuni dati descrittivi in termini di trattamenti, verificarne la liceità, le caratteristiche, la numerosità, latipologia degli interessati, l'identificativo del dossier, ove esistente, oppure la creazione di uno nuovo. Nel caso di atti che si riferiscono a dossier già attivati si dovrà rendere conto del fatto che il dossier è stato aggiornato con i documenti previsti nel processo di Data Protection by Design;
- che sia realizzato all'interno del sistema documentale il Dossier Data Protection per i diversi processi che verranno attivati.
Si ricorda che la gestione del Dossier è finalizzata a rendere agevole l'attività di accountability in quanto terrà traccia di tutti gli adempimenti fatti, di tutte le scelte fatte e delle relative motivazioni.

13.1.1 Mantenimento del registro dei trattamenti

Gli addetti individuati per aree omogenee di azione/funzione all'interno dell'azienda:
a. al momento della predisposizione di atti amministrativi individuano se quell'atto prefigura o interviene in processi che prevedono il trattamento di dati personali, nonché se è necessario prevedere la stipula di appositi *data protection agreement* in base alle regole dedicate ai rapporti DP con terze parti. In tale caso con il supporto degli estensori e dei Data Protection Specialist individuano i trattamenti e ne avviano la registrazione nell'apposito registro, aprono un Dossier Data Protection, rendono conto nell'atto dei nuovi trattamenti e del nuovo Dossier. Nel caso di atti che intervengono successivamente su trattamenti già individuati e/o Dossier già aperti, si procede alla verifica di quanto registrato nel registro dei trattamenti, si aggiorna se del caso il dossier, si da atto, nell'atto, degli avvenuti aggiornamenti.
b. attraverso i Data Protection Specialist e, se ritenuto necessario, consultando il DPO, per tutte le questioni riguardanti l'individuazione dei trattamenti, delle loro caratteristiche e delle azioni da porre in essere per la loro corretta gestione nel tempo.

13.1.2 Richiesta pareri, formulazione e gestione della DPIA

Gli addetti individuati per aree omogenee di azione/funzione all'interno dell'azienda:
a. attraverso il supporto dei Data Protection Specialist della Direzione e per mezzo dell'applicativo dedicato "Richiesta Pareri", possono indirizzare all'attenzione del DPO la richiesta di pareri formali in merito a questioni riguardanti la protezione dei dati
b. attraverso il coinvolgimento dei Data Protection Specialist predispongono nei casi previsti e con il supporto dell' "ufficio del DPO", la DPIA.
c. richiedono il parere del DPO a chiusura della DPIA.
d. aggiornarnano il Dossier Data Protection con la DPIA.

13.2 Monitoraggio Organizzativo e Accountability

Come evidenziato nelle precedenti sezioni elemento fondamentale per la compliance al GDPR è mettere in atto meccanismi organizzativi che rendano l'attività di protezione del dato, una attività, un pensiero corrente che accompagni l'operato di ogni dipendente. Il DPO con il supporto dei referenti interni aziendali e della Direzione dell'azienda provvederà a redigere apposita relazione sull'adeguatezza dell'organizzazione ai compiti derivanti dall'attuazione del GDPR.
Il Titolare e gli addetti devono:
a) in fase di monitoraggio da parte dell'ufficio del DPO, fornire la massima collaborazione tesa ad evidenziare problemi ed ad individuare soluzioni;

b) in fase di segnalazioni da parte di interessati provvedere, con il supporto eventuale del DPO o del suo ufficio, a mettere in atto misure adeguate a rendere conto delle situazioni oggetto di segnalazione ed eventualmente a mettere in atto misure idonee alla risoluzione dei problemi evidenziati;
c) in fase di ispezione o indagine del garante offrire tutta la collaborazione possibile.

13.3 Monitoraggio tecnologico, controllo misure di sicurezza e gestione degli incidenti

Il Monitoraggio tecnologico è in carico al Security Manager che provvede:
a) alla redazione e attuazione di un piano per le verifiche sulle misure di sicurezza messe in atto dal Responsabile IT o di fornitori esterni;
b) alla verifica della rispondenza delle misure di sicurezza in essere alle linee guida emesse dal DPO;
c) alla relazione periodica sulle misure di sicurezza adottate evidenziando punti di criticità e proponendo remediation plan.

La gestione degli incidenti è in carico al Security Manager e/o del Responsabile IT che:
a) registra l'incidente;
b) avvisa il titolare dei trattamenti coinvolti;
c) provvede ad una valutazione dell'incidente in termini di gravità con la collaborazione del dirigente/i coinvolto/i nel trattamento/i;
d) provvede a relazionare al DPO per la decisione relativa alla segnalazione al garante, alla segnalazione agli interessati, alla segnalazione all'autorità giudiziaria se trattasi di atto potenzialmente doloso.

L'azienda deve assicurare:
a) tutte le condizioni idonee, di collaborazione e contrattuali verso fornitori (individuati come Responsabili) al fine di consentire un efficiente ed agevole lavoro del Security Manager;
b) l'attuazione del remediation plan indicato dal Security Manager nei tempi indicati nello stesso;
c) fornire il supporto in caso di segnalazioni di incidenti al fine di comprendere la gravità degli stessi;
d) la tempestiva segnalazione al Security Manager e/o al Responsabile IT della evidenza di incidenti che possono aver coinvolto dati personali.

14 Garanzia dei diritti degli interessati

Al momento della definizione del trattamento il Direttore Generale identifica e mette in atto le procedure idonee a fornire adeguata informativa agli interessati. Per la corretta individuazione dei contenuti e della forma dell'informativa il Direttore Generale si avvale dei fac simili messi a disposizione dall'ufficio del DPO, del supporto dei Data Protection Specialist di direzione o dell'ufficio del DPO.

Gli interessati tramite i punti di contatto pubblicati per l'interlocuzione con il Titolare e il DPO e attraverso specifico modulo effettuano la richiesta. Iò DPO provvede alla risposta e a dare indicazioni alle aree competenti al fine di dare fattiva e tempestiva risposta alle richieste.