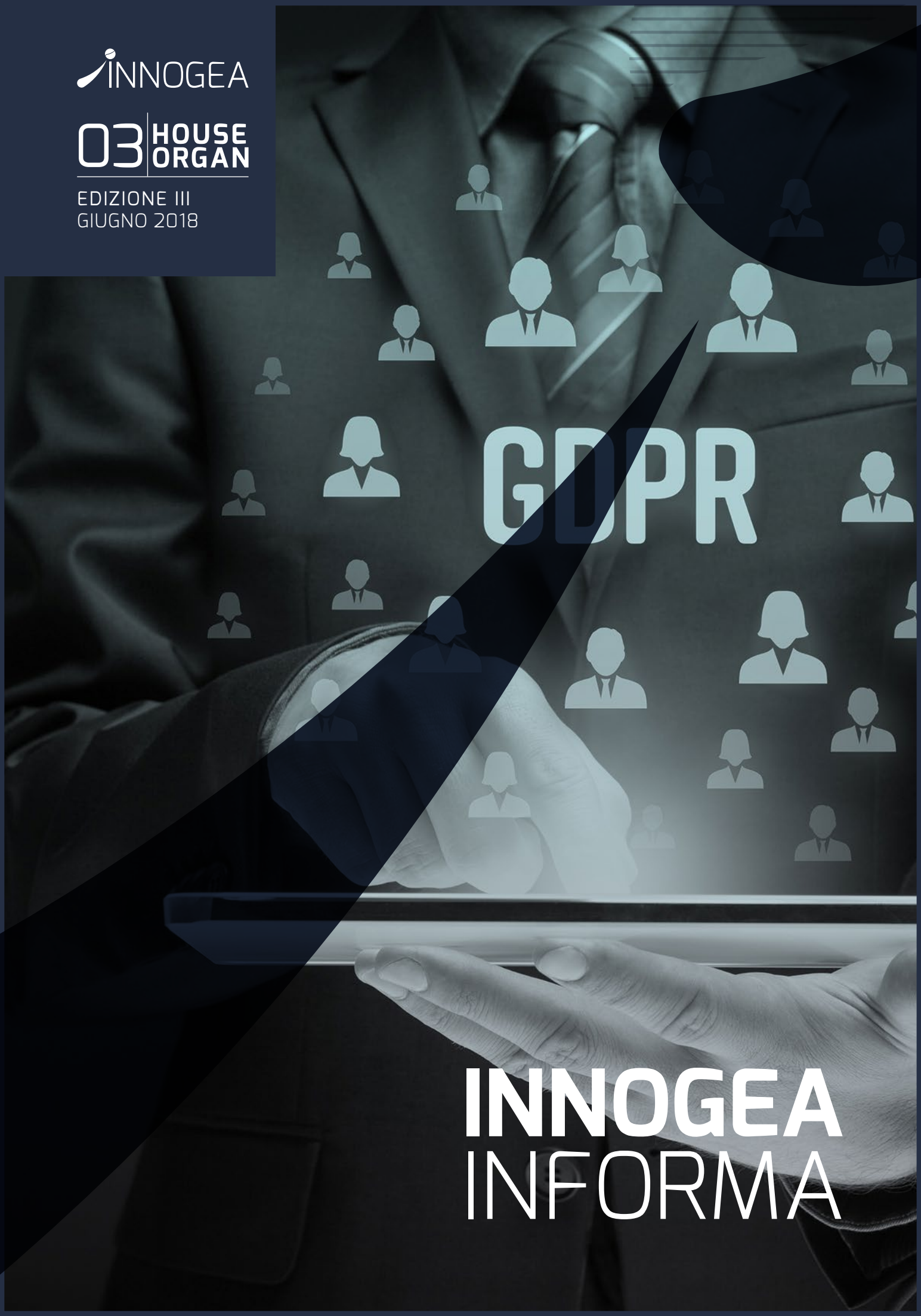
INNOGEA

03 HOUSE ORGAN

EDIZIONE III
GIUGNO 2018

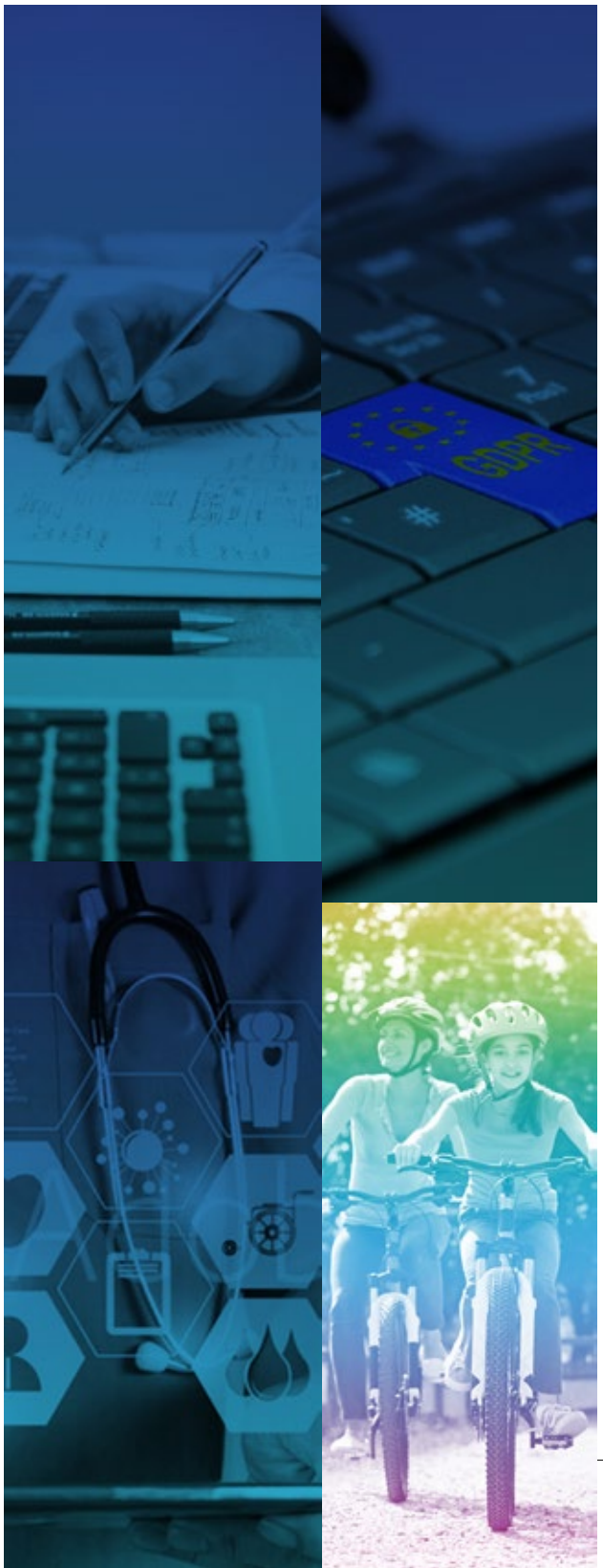


INNOGEA INFORMA

INDEX

HOUSE ORGAN

EDIZIONE III
GIUGNO 2018



EDITORIALE

Marco Lampasona

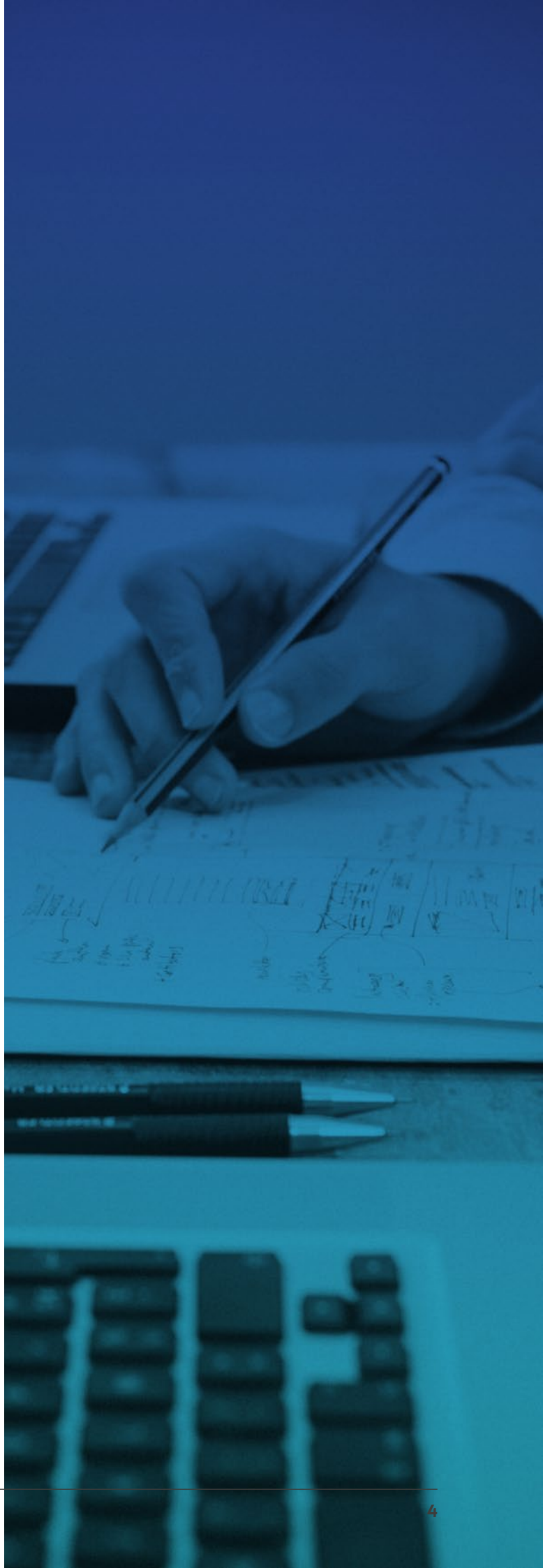
Si chiude un esercizio importante per Innogea che ha visto la nostra società passare da un ambito di azione prevalentemente regionale ad uno nazionale. Abbiamo cercato, in questo percorso intrapreso, di allargare prima di tutto le nostre competenze vista la complessità dettata da un sistema sanitario nazionale che trova specificità differenti a seconda della regione di riferimento in cui ci si trova ad operare.

Il primo semestre 2018 ci ha visto impegnati sul fronte GDPR (Regolamento n. 279/2016). Il tema della privacy per il settore sanitario, da mero adempimento, riteniamo possa diventare una grande opportunità di miglioramento. Una migliore tutela dei dati comporta come conseguenza una migliore conoscenza della propria base assistita con la possibilità di offrire servizi sempre più aderenti alle reali esigenze della comunità.
La tutela dei dati non può che essere inserita nell'ambito di un sistema di gestione aziendale ampio che punti alla qualità dei servizi ed alla sicurezza delle prestazioni sanitarie.
E qui si inserisce l'altro tema che è quello della gestione del rischio in sanità ovvero di tutte quelle prassi, strumenti, comportamenti, dati e informazioni attraverso i quali si possano ridurre gli eventi avversi.
Dopo circa 15 anni di lavoro svolto sulla gestione del rischio e soprattutto sull'innalzamento del livello culturale di tutti i principali stakeholders, l'evento avverso ci sembra più collegato a un fallimento del sistema gestionale - inteso come insieme di organizzazione e tecnologia - che ad un errore comportamentale.
In questo numero, in particolare, parleremo della responsabilità medica, che ha investito il complesso sistema del servizio sanitario nazionale provocando una profonda frattura nell'alleanza terapeutica tra medico e paziente, sfociata un anno fa nella promulgazione della legge n. 24/2017, più nota come "Legge Gelli".
Per ottemperare a tale disposto il professionista sanitario sarò tenuto a gestire e a trasferire una mole cospicua di informazioni per via digitale. Tra queste i dati relativi ai risarcimenti effettuati negli ultimi 5 anni presso ciascuna struttura (da pubblicarsi sul sito internet della stessa) e quelli inerenti la gestione del rischio clinico (inclusi gli eventi avversi).
Tutta questa attività viene ora ad integrarsi il GDPR, che impone a tutti i soggetti che debbano in qualunque modo gestire, conservare, trasferire o trattare dati personali di adottare un'articolata politica di risk management, allo scopo di garantire la propria conformità ai requisiti di sicurezza previsti dal Regolamento stesso.
A completare gli articoli di questo numero c'è un interessante approfondimento sulla corretta allocazione del budget per le strutture convenzionate. Sandro Siniscalchi, Partner di Innogea, ci spiegherà la logica che consente alle aziende di rendere efficace questo processo.

Infine vi racconteremo un progetto di "social responsability" giunto alla sua seconda edizione ideato e fortemente voluto da Innogea. Si tratta del progetto di valorizzazione del Parco Reale della Favorita meglio conosciuto come "La Domenica Favorita" (www.ladomenicafavorita.com); Anche nel 2018 oltre 60 mila persone hanno partecipato all'evento. Vi riportiamo uno stralcio di articolo che è stato pubblicato su "La Repubblica" che spiega da dove nasce l'idea.

Buona Lettura
Marco Lampasona

L'autore: Marco Lampasona
È stato Direttore Generale del Dipartimento Studi Territoriali di Palermo, esperto del Ministro dello Sviluppo Economico, consulente della Presidenza del Consiglio e componente dell'Unità di Verifica degli Investimenti Pubblici. Ha maturato un expertise verticale in Business Management. Oggi è partner di innogea.



L'applicazione del GDPR nelle organizzazioni sanitarie e l'integrazione con il sistema di gestione per la qualità

Filippo Castelli

Come ormai tutti sappiamo dal 25 maggio 2018 è entrato in piena efficacia il Regolamento generale sulla Protezione dei dati Regolamento (UE) 2016/679 (GDPR). In questi mesi abbiamo imparato a familiarizzare con i nuovi concetti, le nuove figure, i nuovi strumenti di analisi e valutazione richiesti dal GDPR (il registro dei trattamenti, la DPIA, il DPO etc.). Ovviamente, anche in considerazione delle sanzioni previste, la conformità viene prima di ogni altra cosa, vi è però una grossa opportunità che a nostro avviso va colta per ottenere dal GDPR e dalla sua applicazione, il massimo dei benefici a livello organizzativo e per interpretarlo in ottica opportunamente dinamica evitando che quanto di buono venga fatto in sede di prima applicazione, sia poi vanificato. Tale opportunità è rappresentata dal dotare l'organizzazione di un sistema di gestione per la data protection che copra tutti gli aspetti del GDPR integrando lo stesso in maniera intima e concreta con l'esistente sistema di gestione per la qualità che ogni organizzazione sanitaria o sociosanitaria possiede. Ma come si applica il GDPR nelle strutture sanitarie e sociosanitarie e come si può integrare il modello organizzativo per la *data protection* ai SGQ?

La prima considerazione va fatta circa l'ambito di applicazione. Il regolamento si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi. In una struttura sanitaria, rientrano in tale fattispecie, ad esempio: I dati personali dei lavoratori; gli archivi cartacei delle cartelle personali dei lavoratori; i dati personali dei pazienti/ospiti; gli archivi cartacei di cartelle cliniche; i dati di fornitori di prodotti, servizi e di appaltatori. Tra questi ultimi bisogna individuare quelli che trattano per conto del titolare, dati personali, in quanto possibili candidati al ruolo di responsabili (esterni) del trattamento.

Per una corretta gestione delle informative e dei consensi al trattamento occorre a nostro avviso redigere una specifica procedura con lo scopo di definire le modalità e le responsabilità per:

- La verifica della liceità dei trattamenti;
- La definizione delle informative al trattamento e delle relative modalità e tempi di somministrazione;
- La definizione dei moduli per l'acquisizione, ove richiesti, dei consensi informati specifici per le attività di trattamento;
- Le modalità ed i tempi di conservazione della documentazione.

A corredo della procedura vanno create e codificate informazioni documentate relative ai moduli di informativa e consenso.

In un SGQ basato sulla norma UNI EN ISO 9001:2015 tale procedura può trovare integrazione, ad esempio con la procedura di acquisizione e gestione del consenso informato alle prestazioni diagnostico-terapeutico-assistenziali, parte sostanziale dell'applicazione del punto 8.5 della norma citata.

Particolare attenzione va prestata al concetto di profilazione (art. 22) e verificare l'applicazione corretta di concetti quali: analisi del rendimento professionale, analisi di affidabilità o comportamento, diritto degli interessati di non essere sottoposti a una decisione basata unicamente su un trattamento automatizzato e che produca effetti giuridici che li riguardano.
In generale, nella nostra esperienza, nelle strutture sanitarie non si esegue attività di profilazione così come definita nel documento *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, tuttavia va verificata, specialmente nelle strutture maggiormente informatizzate ed evolute l'attività di *data collecting e reporting* finalizzata al conferimento ed aggiornamento dei *privileges* previsti dagli standard Joint Commission International recepiti con *DECRETO 12 agosto 2011. Approvazione dei nuovi standard Joint Commission International per la gestione del rischio clinico*.

Il GDPR stabilisce negli artt. 11 e 12, le modalità per l'esercizio di tutti i diritti da parte degli interessati. A tale riguardo, a nostro avviso, sarebbe opportuno redigere una procedura con lo scopo di definire le modalità e le responsabilità per:
- La gestione delle richieste, da parte degli interessati di esercizio dei propri diritti relativi al trattamento dei propri dati;
- La gestione delle notifiche;
- La rendicontazione.

In un SGQ basato sulla norma UNI EN ISO 9001:2015 tale procedura può trovare integrazione, ad esempio con la procedura di comunicazione, partecipazione e consultazione, parte sostanziale dell'applicazione del punto 7.4 della norma citata. A corredo della procedura vanno creati documenti specifici per il monitoraggio delle richieste degli interessati al trattamento e per la notifica ai destinatari. Sarebbe inoltre opportuno monitorare specifici indicatori relativi ai tempi medi di risposta agli interessati, che dovrebbero peraltro essere inseriti anche come livello standard di prestazione nella carta dei servizi della struttura.

È necessario redigere uno specifico organigramma della *data protection* da affiancare agli esistenti organigrammi. Appare opportuno revisionare il mansionario aziendale con lo scopo di definire le responsabilità e le attività connesse con i ruoli più significativi ed i profili personali e professionali richiesti ai fini del conseguimento della compliance al GDPR. L'organigramma definirà chiaramente ruoli quali: Titolare, Contitolare, Rappresentante del Titolare, DPO, Delegati Interni, Responsabili (esterni) incaricati del trattamento etc. Per ciascuno di essi occorrerà predisporre e documentare specifico documento di designazione e nomina. Ovviamente, per le responsabilità concomitanti sarà necessario arricchire le già esistenti *job description* non tralasciando di farle sottoscrivere nuovamente agli interessati. Non sembra necessario spendere ulteriori parole ai fini della valutazione dell'obbligatorietà o meno della nomina del DPO da parte delle strutture sanitarie. Come chiarito dalla linea guida *WP 243 - Linee-guida sui responsabili della protezione dei dati (RPD)* dove si legge quanto segue:
A ogni modo, il Gruppo di lavoro raccomanda di tenere conto, in particolare, dei fattori elencati nel prosieguo al fine di stabilire se un trattamento sia effettuato su larga scala:
- ***Il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;***
- *Il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;*
- *La durata, ovvero la persistenza, dell'attività di trattamento;*
- *La portata geografica dell'attività di trattamento.*

Alcuni esempi di trattamento su larga scala sono i seguenti:

• *Trattamento di dati relativi a pazienti svolto da un ospedale nell'ambito delle ordinarie attività.*

Occorre infine, una volta individuati e inseriti nell'organigramma della *data protection* i responsabili (esterni) del trattamento, redigere una specifica istruzione di lavoro con lo scopo di assolvere ai dettami del paragrafo 3 dell'art. 28 del GDPR che tra l'altro richiede che il responsabile del trattamento *tratti i dati personali soltanto* ***su istruzione documentata*** *del titolare del trattamento*. Ovviamente, tale istruzione non soltanto va predisposta per ciascun responsabile, ma ne va richiesta ed ottenuta la sottoscrizione per presa visione ed accettazione. Pur non prevedendo espressamente la figura dell'incaricato del trattamento (ex art. 30 Codice), il GDPR non ne esclude la presenza in quanto fa riferimento a *"persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile"*. L'articolo 29 del GDPR a tale riguardo prevede che. "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**. Occorre pertanto a nostro avviso pianificare senza indugio, laddove non effettuato, un corso di formazione e addestramento sulle modalità di trattamento dei dati per tutto il personale interessato.

La dovuta attenzione va data ai concetti di *Data protection by default and by design* (si veda art. 25 del GDPR) intesa come la necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili "al fine di soddisfare i requisiti" del regolamento e tutelare i diritti degli interessati. Tutto questo deve avvenire a monte, prima di procedere al trattamento dei dati vero e proprio ("sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso", secondo quanto afferma l'art. 25, paragrafo 1 del regolamento) e richiede, pertanto, un'analisi preventiva e un impegno applicativo da parte dei titolari che devono sostanziarsi in una serie di attività specifiche e dimostrabili. A tale riguardo è opportuno, a nostro avviso, predisporre istruzioni specifiche per disciplinare aspetti critici dal punto di vista della data protection by default e by design quali, ad esempio: il setup e la dismissione fisica e logica di una macchina, la gestione delle credenziali di accesso ed il setup dei profili autorizzativi etc.

Fondamentali sono le attività di valutazione dei rischi inerenti il trattamento ovvero impatti negativi sulle libertà e i diritti degli interessati; tali impatti devono essere analizzati attraverso un apposito processo di valutazione tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative che il titolare ritiene di dover adottare per mitigare tali rischi. In tale ottica si colloca il Data Protection Impact Assessment (DPIA). La DPIA va effettuata quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, **può presentare un rischio elevato per i diritti e le libertà delle persone fisiche**. La DPIA è richiesta in particolare in caso di trattamento, su larga scala, di categorie particolari di dati personali (tra cui i dati sullo stato di salute degli interessati). Ne deriva che nelle strutture sanitarie e sociosanitarie per cui si configuri il trattamento "su larga scala" la DPIA va effettuata per il trattamento dei dati dei pazienti/ospiti. Occorre al riguardo mettere a punto un'apposita procedura con lo scopo di definire le responsabilità e le attività per la conduzione della DPIA e per l'eventuale consultazione preventiva.

Tutti i titolari e i responsabili di trattamento, eccettuati gli organismi con meno di 250 dipendenti ma solo se non effettuano trattamenti a rischio (si veda art. 30, paragrafo 5), devono

tenere un registro delle operazioni di trattamento i cui contenuti sono indicati all'art. 30. Una specifica procedura dovrà pertanto definire le responsabilità e le attività per:
• La compilazione e l'aggiornamento del registro delle attività di trattamento;
• La verifica della compilazione da parte dei responsabili del trattamento del loro registro;
• La messa a disposizione del registro alle autorità competenti.
Il registro dei trattamenti sarà redatto e aggiornato come documento di registrazione.

Passaggio determinante, nelle attività che da porre in essere è l'effettuazione di un assessment di vulnerabilità del sistema informatico ai fini della valutazione dei rischi e per pianificarne il miglioramento. Nell'ambito di tale assessment dovrebbero essere esaminati aspetti quali:
• Esistenza censimento delle risorse e sistemi in rete;
• Esistenza elenco e mappa degli applicativi in uso del sistema informativo aziendale e documentazione dell'allocazione fisica dei dati sui server;
• *IDM, Logging e Single Sign On*;
• Esistenza di documentazione tecnica della struttura del Database per applicativo;
• Esistenza procedure formalizzate di *backup e restore* per singolo applicativo/Database;
• Esistenza di procedure di gestione delle basi dati (patching, manutenzione, etc.);
• Valutazione della possibilità di accessi non autorizzati ai sistemi e al db, copia non autorizzata di dati, manomissione e falsificazione dati;
Inventario e assessment delle tecnologie in essere;
• Esistenza di procedure/sistemi per *logging* degli eventi e/o degli amministratori;
• Pseudonimizzazione ed *encryprtion*;
• *Penetration test*.
In genere in un SGQ la procedura di gestione del sistema informativo è già esistente e trova integrazione e correlazione con la procedura di gestione delle risorse di cui al punto 7.1 della norma ISO 9001:2015. È tuttavia opportuno farne oggetto di revisione al fine di verificare che contenga tutti gli elementi necessari elencati e ne disciplini attività e responsabilità.

A partire dal 25 maggio 2018, tutti i titolari dovranno notificare all'Autorità di controllo le violazioni di dati personali di cui vengano a conoscenza, entro 72 ore e comunque "senza ingiustificato ritardo", ma soltanto se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati (si veda considerando 85). Cosa si intende per violazione dei dati personali? Di chi è la responsabilità della loro individuazione? Cosa bisogna fare? Ovviamente, anche in questo è opportuno pianificare in una specifica procedura le responsabilità e le attività per:
• L'individuazione dei *data breach*;
• La comunicazione all'autorità;
• La comunicazione all'interessato;
• L'analisi delle cause e la gestione delle azioni correttive.
In un SGQ basato sulla norma UNI EN ISO 9001:2015 tale procedura può trovare integrazione con la procedura di gestione delle non conformità caposaldo del sistema e rispondente al punto 10.2 della norma.

Al termine delle attività di integrazione dei nuovi adempimenti all'interno delle normali attività dell'organizzazione pianificandole con opportune procedure integrate al sistema di gestione per la qualità ed implementandole con la necessaria attività di formazione, occorre garantire che la ciclicità del sistema disegnata sulla base del ciclo di Deming abbracci anche la Data protection:
• Prevedendo obiettivi specifici di miglioramento anche in termini di data protection e programmi per il loro raggiungimento;

• Integrando alle attività di auditing interno anche le verifiche a cura del team di audit o del DPO in materia di data protection;
• Prevedendo che in sede di riesame da parte della Direzione (o in sede analoga) vengano valutate le performance specifiche dell'organizzazione anche in tema di data protection e si prendano le opportune decisioni allocando risorse ai fini del miglioramento.

L'autore: Filippo Castelli
Consulente di oltre 25 strutture sanitarie su tematiche legate alla compliance ed in particolare al risk management, all' accreditamento di eccellenza ed istituzionale. Oggi ricopre il ruolo di Responsabile della Divisione Operation di Innogea.

I requisiti della Legge Gelli alla luce del GDPR.

Cinzia Altomare

La crisi della responsabilità medica che ha investito il complesso sistema del servizio sanitario nazionale, provocando una profonda frattura nell'alleanza terapeutica tra medico e paziente, è sfociata un anno fa nella promulgazione della legge n. 24/2017, più nota come "Legge Gelli".

Il provvedimento completa, amplia e rende più omogenea la precedente legislazione in materia di responsabilità sanitaria. Suoi scopi dichiarati, la riduzione del contenzioso legale esistente in materia di responsabilità medica e del cosiddetto fenomeno della *Medicina Difensiva*, indicato dal Ministero della Sanità come causa principale di un eccesso di spesa pubblica ammontante a svariati miliardi di euro, nonché la creazione di un ambiente di lavoro più sicuro e sereno per i professionisti del comparto, il tutto con l'intento di migliorare la qualità del servizio sanitario nazionale, garantendo al cittadino il rispetto del suo diritto costituzionale alla salute.

La nuova normativa prevede anche un uso intensivo degli strumenti informatici: per ottemperare al disposto della legge Gelli, infatti, ogni professionista sanitario è oggi tenuto a gestire e trasferire una mole cospicua di informazioni per via digitale. Tra queste, i dati relativi ai risarcimenti effettuati negli ultimi 5 anni presso ciascuna struttura (da pubblicarsi sul sito internet della stessa) e quelli inerenti la gestione del rischio clinico (inclusi gli eventi avversi), da trasferirsi mediante procedura telematica unificata a livello nazionale, all'Osservatorio Nazionale delle buone pratiche sulla sicurezza in sanità.

Tutta questa attività viene ora ad integrarsi con la gestione del rischio imposta dalla nuova normativa europea sul trattamento dei dati personali, come da Regolamento n. 279/2016, entrata definitivamente in vigore nel nostro paese il 25 maggio scorso. Si tratta del GDPR (General Data Protection Regulation), che impone a tutti i soggetti che debbano in qualunque modo gestire, conservare, trasferire o trattare dati personali di adottare un'articolata politica di risk management, allo scopo di garantire la propria conformità ai requisiti di sicurezza previsti dal Regolamento stesso.

La protezione dei dati delle persone fisiche costituisce infatti un diritto sancito dall'articolo 8 della Carta dei diritti fondamentali e dall'articolo 16 del Trattato sul funzionamento dell'Unione Europea ed è vitale che le norme previste per la loro tutela siano improntate al pieno rispetto delle libertà di chi li possiede. Per quanto attiene al comparto sanitario, la nuova normativa impone di prestare particolare attenzione alla tutela della privacy, meritando **i dati sanitari** (il cui concetto viene per la prima volta specificamente introdotto dal Regolamento) una **tutela rafforzata**, proprio per il coinvolgimento di diritti di rilievo costituzionale.

Già a partire dal Codice della Privacy, giurisprudenza e dottrina hanno operato delle distinzioni tra dati personali, sensibili e sensibilissimi, collocando i dati sanitari, per la loro stessa natura, nella categoria dei **dati sensibilissimi** e facendo-

ne oggetto di protezione rafforzata, per impedirne l'uso improprio o illegittimo. Il Considerando n. 35 del Regolamento chiarisce ora il concetto di dati riguardanti la salute della persona e fornisce specifiche definizioni:

- **Dati personali:** qualsiasi informazione riguardante una persona fisica direttamente o indirettamente identificabile (nome, ubicazione, elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale);
- **Dati genetici:** informazioni sulle caratteristiche genetiche ereditarie o acquisite di una persona fisica (fisiologia e salute), che risultano n particolare dall'analisi di un suo campione biologico;
- **Dati biometrici:** informazioni ottenute da un trattamento specifico e relative alle caratteristiche fisiche, fisiologiche o comportamentali, come foto e dati dattiloscopici;
- **Dati relativi alla salute:** informazioni personali attinenti alla salute fisica o mentale di una persona, compresa la prestazione di servizi di assistenza sanitaria, che rivelino informazioni sul suo stato di salute.

La nuova disciplina amplia il novero degli obblighi in capo a tutti coloro che trattino dati personali, ma pone nelle loro mani il compito di individuare le misure che riducano il rischio di violazioni, attraverso l'introduzione del concetto di **accountability** di tutti i soggetti interessati al trattamento stesso.

In un certo senso, viene qui capovolto il principio sinora adottato, di imporre dall'alto il rispetto di una particolare normativa, valida per tutti: dal momento che ogni tipo di attività prevede caratteristiche uniche e differenti e può necessitare di un diverso tipo di approccio, il dovere di adottare le procedure più adatte alla bisogna viene posto in capo alle figure chiave che il Regolamento impone di individuare all'interno di ciascuna azienda.

Sono questi il **Titolare ed il Responsabile del Trattamento**, che saranno tenuti a:

a) garantire un livello di sicurezza adeguato al tipo ed alla modalità del trattamento effettuato;

b) assicurare la riservatezza, l'integrità, la disponibilità e la flessibilità di sistemi e procedure per la gestione dei dati personali;

c) garantire il ripristino tempestivo dell'accesso ai dati personali, in caso di incidente tecnico;

d) fornire prova dell'intero processo, dimostrando che le scelte operate sono appropriate ed efficaci;

e) garantire che chiunque abbia accesso ai dati trattati sia stato adeguatamente istruito in tal senso.

Queste figure possono essere affiancate da una terza, costituita dal **Data Privacy Officer** (DPO), il quale può anche essere un soggetto esterno all'azienda ed ha il ruolo di referente diretto del Garante. La sua nomina è obbligatoria per gli Enti Pubblici e per le imprese che trattino un rilevante numero di dati, oppure tipologie di dati considerate per loro natura a rischio, com'è il caso dei dati sanitari.

È questa una nuova figura professionale, dotata di competenze giuridiche, informatiche ed organizzative, che svolge un ruolo di controllo e supporto strategico per le decisioni operative del Titolare.

Il Regolamento prevede che ciascuna azienda debba munirsi di misure di sicurezza tanto più sofisticate, quanto più sensibili saranno i dati personali gestiti. Ciò implica la *pseudonimizzazione* e *cifratura* dei dati, la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento, nonché, come abbiamo accennato, la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati, in caso di incidente. È inoltre obbligatoria l'istituzione di una procedura per testare e verificare l'efficacia delle misure tecniche ed organizzative adottate.

In pratica, si tratta di porre in atto le procedure più adatte e di prevederne anche il controllo continuo nel tempo, nel rispetto degli oneri

imposti dalla nuova normativa, come definire i tempi di conservazione dei dati ed indicare la loro provenienza, comunicare tempestivamente al Garante le violazioni dei propri database, nonché predisporre il documento di valutazione di impatto del trattamento dei dati personali (PIA, o Privacy Impact Assessment), elaborando un sistema documentale di gestione della privacy contenente tutti gli atti aggiornati per soddisfare i requisiti di conformità al Regolamento ed istituendo un Registro del trattamento dei dati, nel quale siano tracciabili e documentabili tutte le operazioni di trattamento.

Le misure difensive previste in ottemperanza al GDPR dovranno essere strutturate nelle aziende sanitarie di ogni ordine, sia attraverso modelli operativi di programmazione e di formazione del personale, che attraverso sistemi di sicurezza tecnologici.
Vengono identificati come possibile ambito di violazione di dati, la pratica della telemedicina, l'errata consegna del dato (invio elettronico del referto al destinatario sbagliato) e la sua errata pubblicazione (informazioni sanitarie erroneamente diffuse sul sito internet), nonché la mancata o errata distruzione dei dati, dopo il loro uso.
Anche l'uso di devices personali per registrare/copiare dati sensibili costituisce una palese violazione del Regolamento: bisognerà quindi dedicare particolare attenzione alla pratica di copiare i dati su chiavetta o laptop personali, da parte di dipendenti ed operatori: l'*insider misuse* è infatti segnalato nel *rapporto Clusit* come una delle più comuni cause di violazione dei dati sanitari in Italia.
Sotto questo profilo, la formazione riveste un ruolo fondamentale nella gestione della privacy. Già gli artt. 33 e 35 del Codice della Privacy prevedevano che il trattamento dei dati personali fosse effettuato solo a condizione che il personale fosse adeguatamente istruito. Ora è certo che il grado di formazione debba essere adeguato alla tipologia dei dati trattati e l'omissione di un'adeguata formazione e istruzione di tutti gli incaricati del trattamento costituirà a tutti gli effetti un'omissione di misure minime di sicurezza.
L'importanza di un adeguato training di tutti gli operatori sanitari è anche dettata dal fatto che in quest'ambito le attività che prevedono l'uso di dati personali sono piuttosto diffuse e vengono effettuate a tutti i livelli. Quasi ogni operatore, di fatto, può trovarsi nella necessità di interfacciarsi col paziente ed in questo caso assume un ruolo chiave la qualità delle comunicazioni fornite all'interessato.
Il trattamento di dati personali, soprattutto se sanitari, è infatti considerato lecito solo previa informativa e consenso dell'interessato. Il Regolamento prevede inoltre che il consenso prestato in sanità debba avvenire per mezzo di una dichiarazione inequivocabile ed esplicita. Tale consenso può essere revocato in ogni momento e vi è obbligo di informazione preventiva proprio sulla sua revocabilità.
In ambito sanitario, dunque, Titolari e Responsabili del trattamento, nonché relativi DPO, dovranno misurarsi con l'obbligo di gestire e proteggere nel migliore dei modi una serie di documenti particolari che caratterizzano l'attività del comparto e che assumono un'importanza centrale nell'era della cosiddetta Sanità Elettronica o Digitalizzata, quali il Fascicolo Sanitario Elettronico (FSE), il Dossier Sanitario, la Cartella Clinica Elettronica (CCE) ed il Referto On-Line.
C'è infine da rilevare come i dati sanitari *(o PHI - Protected Health Information)* rappresentino una vera miniera d'oro per i cyber criminali, che li rivendono sul mercato nero per favorire frodi o altre attività criminose.
Secondo il primo *Verizon Protected Health Information Data Breach Report*, pubblicato dal colosso americano della comunicazione, ben 18 aziende sanitarie su 20 sono state interessate da furti di dati personali. Le violazioni confer-

te hanno coinvolto oltre 392 milioni di record in 1.931 incidenti occorsi in 25 nazioni differenti, incluse alcune europee, come la Germania. In seguito a tale escalation l'FBI ha diffuso un allarme per gli operatori sanitari, evidenziando la possibilità di un incremento delle intrusioni informatiche in tale settore.

Non desta alcuna meraviglia, quindi, che il nuovo Regolamento europeo attribuisca tanta importanza alla protezione di dati così sensibili diventando essi stessi oggetto di gestione del rischio.

L'autore: Cinzia Altomare
Responsabile RC Medica presso Verspieren Italia

La corretta allocazione del budget per le Strutture Sanitarie Convenzionate.

Sandro Siniscalchi

Tra gli obiettivi di un manager di in un'azienda appartenente ad un qualsiasi settore industriale c'è, indubbiamente, la massimizzazione dei ricavi. Le regole cui deve sottostare un manager di una struttura sanitaria sono, invece, ben diverse. I ricavi dell'azienda non sono massimizzabili semplicemente rispondendo in maniera efficace ed efficiente alla domanda di salute presente sul territorio, questi sono contingentati dal budget assegnato dal Sistema Sanitario Nazionale. Il manager ha quindi a disposizione una risorsa scarsa (il budget) che deve allocare in maniera oculata tra tutte le unità funzionali presenti in azienda al fine di massimizzarne il risultato operativo. Come può, quindi, un manager allocare correttamente il budget a propria disposizione? Quali sono le valutazioni necessarie a questa allocazione?

Si tratta, chiaramente, di valutazioni che non si fermano al mero aspetto economico ma che abbracciano l'intera organizzazione della struttura. Se da un lato è necessario rispettare le cogenze imposte dall'Azienda Sanitaria Provinciale/ Locale di riferimento dall'altro bisogna anche valutare le potenzialità della propria struttura organizzativa e la domanda di salute presente sul territorio in cui si opera.

Non sempre i manager hanno a disposizione i dati necessari alle valutazioni che permettono la corretta assegnazione del budget, a tal fine è necessario che la struttura sanitaria sia dotata di:

- Una cartella clinica informatizzata che permetta la rilevazione del c.d. Costo Paziente;
- Un sistema di controllo di gestione che permetta la valutazione di un conto economico a margini per le singole unità funzionali.

Questa *Dotazione Minima* permetterà al manager di valutare correttamente i dati a propria disposizione, in particolare sarà necessario effettuare la prima importante valutazione:

Qual è il margine lordo delle unità funzionali?

La risposta a questa domanda permetterà al management di capire, in maniera precisa e puntuale, quanto costa produrre fatturato in una determinata unità funzionale.

Il margine lordo rappresenta la differenza tra i ricavi ed i costi diretti variabili imputabili specificatamente all'unità funzionale in esame. Se, ad esempio, la Chirurgia Generale ha un margine lordo del 50% significa che la produzione di € 100.000,00 di Fatturato costa € 50.000,00, qualora l'Urologia avesse un margine lordo di contribuzione pari al 65% ciò significa che la produzione di €100.000,00 costa € 35.000,00. È quasi spontaneo affermare che è *più conveniente* assegnare più budget all'unità funzionale di Urologia, piuttosto che alla Chirurgia Generale. Tuttavia è necessario considerare molti altri fattori che influenzano la produzione tra questi:

- Le equipe possono rispondere efficacemente ad un eventuale incremento di produzione?
- Abbiamo già saturato la domanda di salute per le prestazioni dell'UF di urologia nel territorio di riferimento?
- Il decremento del budget all'UF di Chirurgia Generale ci permetterebbe comunque di rispon-

dere alle cogenze dell'azienda sanitaria provinciale/locale?

• Cosa accade alla struttura organizzativa qualora decidessimo di incrementare la produzione in Urologia? Dobbiamo asssumere nuove risorse? Possiamo riallocare risorse che abbiamo già in organico in maniera più efficiente?

• Come cambierà l'utilizzo della Sala Operatoria?

La risposta a queste domande comporta una complessa, ma molto interessante, analisi *What If*. La variazione del budget assegnato a due UF non comporta cambiamenti solo nella struttura di quest'ultime bensì sull'intera organizzazione. La complessità di queste analisi permette di comprendere che il controllo di gestione non è uno strumento finalizzato esclusivamente al monitoraggio dell'andamento economico di un'azienda sanitaria, ma si tratta di un più ampio strumento che permette di controllare l'efficienza, l'efficacia e la bontà della propria organizzazione.

Una corretta allocazione del budget tra le unità funzionali presenti in una struttura sanitaria può comportare un miglioramento stimabile, secondo l'esperienza affinata negli anni di consulenza presso le strutture sanitarie clienti di Innogea, tra il 10% ed il 20% del risultato operativo della gestione ordinaria che, se rapportato al budget assegnato, rappresenta indubbiamente un notevole miglioramento in termini di valore assoluto.

L'autore: Sandro Siniscalchi

È esperto in materia di Controllo di Gestione e consulenza direzionale sia in strutture sanitarie che in aziende appartenenti ad altri settori industriali con un esperienza ventennale. È stato consigliere delegato di strutture sanitarie accreditate SSN occupandosi di gestione del personale, acquisti ed amministrazione e contabilità ed amministratore delegato di società di franchising su scala nazionale. In Innogea è Partner e CFO, ricopre inoltre il ruolo di responsabile della divisione Management.

La seconda edizione de “La Domenica Favorita”: un progetto di social responsability

Marco Lampasona

Innogea continua ad essere impegnata sul sociale con lo scopo di valorizzare il proprio territorio di riferimento, la Sicilia, attraverso progetti che puntano ad unire la cultura, la natura e lo sport.
Anche quest’anno abbiamo sostenuto “La Domenica Favorita” con il contributo dell’amministrazione comunale di Palermo giunta alla sua seconda edizione, ed avviato un nuovo progetto finalizzato a fare conoscere la Sicilia attraverso la bici.
Di questa ultima iniziativa, denominata il Giro della Sicilia (www.girodellasicilia.com) vi parleremo nel prossimo numero.

Di seguito un estratto dell’ articolo del nostro Direttore Generale pubblicato su La Repubblica Palermo del 14 aprile 2018

Ho sempre pensato, sicuramente indotto dalla cultura cattolica nella quale sono cresciuto, che non valorizzare un “talento” sia un peccato. Da siciliano ne ho visti tanti talenti “sprecati”; la Sicilia ne è piena.

Il Parco della Favorita per me è sempre rientrato in tale novero. Tanti palermitani lo attraversano ogni giorno senza neanche rendersi conto di quello che c’è dentro; notano, magari, giustamente le tante cose che non vanno - tipico della nostra cultura - senza apprezzare, nella giusta misura, la ricchezza naturalistica e culturale di questo polmone verde che si trova ad appena 2 km dal centro della città.
Ed ecco la scintilla: provare a fare qualcosa piuttosto che rimanere in attesa.
L’idea del **“La Domenica Favorita”** nasce da queste premesse e dal seguente presupposto su cui ci siamo basati: il miglior modo di valorizzare un bene è quello di farlo conoscere consentendone la fruizione;
Concetto tanto semplice quanto banale, quello sopra riportato, ma spesso sottovalutato.

Commento

FAVORITA, UN PARCO “VIVO” E NON SOLO LA DOMENICA

Marco Lampasona

Ho sempre pensato, sicuramente indotto dalla cultura cattolica nella quale sono cresciuto, che non valorizzare un “talento” sia un peccato. Da siciliano ne ho visti tanti, di talenti “sprecati”: la Sicilia ne è piena. Il parco della Favorita per me è sempre rientrato in tale novero. Tanti palermitani lo attraversano ogni giorno senza neanche rendersi conto di quello che c’è dentro. Notano, magari, giustamente le tante cose che non vanno – tipico della nostra cultura – senza apprezzare, nella giusta misura, la ricchezza naturalistica e culturale di questo polmone verde che si trova ad appena due chilometri dal centro della città. Ed ecco la scintilla: provare a fare qualcosa, piuttosto che rimanere in attesa. L’idea de “La Domenica Favorita” nasce da queste premesse e da questo presupposto: il miglior modo di valorizzare un bene è quello di farlo conoscere consentendone la fruizione. Concetto tanto semplice quanto banale, ma spesso sottovalutato. Certamente la chiusura al traffico veicolare non era sufficiente. Allora abbiamo pensato che sarebbe bastato, semplicemente, proporre in maniera organizzata tutte le attività che tipicamente si possono fare in un parco: attività ludiche, culturali e sportive a impatto zero. Da lì in poi è stato tutto meno complesso di quello che appare: trovare amici con cui condividere e realizzare l’idea, Nicola Tricomi e Fabio Corsini, e lavorare duramente sognando domeniche palermitane diverse in cui ognuno, indipendentemente dall’età, potesse andare al parco per divertirsi, mettersi in relazione e condividere quanto di bello la Favorita offre. A questo punto mancava solo un piccolo dettaglio: presentare e condividere il progetto con l’amministrazione comunale e ingaggiare tutti i soggetti pubblici e privati per creare un palinsesto di eventi. Cosa non di poco conto... Quella che ci sembrava la parte più difficile è stata invece la più semplice. Abbiamo trovato un entusiasmo disarmante da parte di tutti, in primis da parte del sindaco Orlando e di tutta l’amministrazione comunale. Il nostro piccolo merito, se ne dobbiamo trovare uno, è stato quello di mettere tutti in relazione in un circolo virtuoso, per una causa nobile. Il sogno finale è quello di avere un parco “vivo”, ricco di attività sociali ed economiche; un’area che possa offrire intrattenimento e opportunità di lavoro. Spero che un giorno, quando i miei figli diventeranno adulti, non ci sarà più solamente “La Domenica Favorita” ma ci saranno anche il Lunedì, il Martedì, il Mercoledì, il Giovedì, il Venerdì, il Sabato Favorita. Chi vivrà vedrà.

“Capimmo che la chiusura al traffico non bastava Servivano attività ludiche culturali e sportive”

L’articolo pubblicato su La Repubblica del 14 aprile 2018

Certamente la chiusura al traffico veicolare non era sufficiente; ed allora abbiamo pensato che sarebbe bastato, semplicemente, proporre in maniera organizzata tutte le attività che tipicamente si possono fare in un Parco: attività ludiche, culturali, e sportive a impatto zero.
Da lì in poi è stato tutto meno complesso di quello che appare: trovare degli amici con cui condividere e realizzare l'idea, Nicola Tricomi e Fabio Corsini, e lavorare duramente sognando delle domeniche palermitane diverse in cui ognuno, indipendentemente dall'età, potesse andare al Parco per divertirsi, mettersi in relazione e condividere quanto di bello la Favorita offre.
A questo punto, mancava solo un piccolo dettaglio: presentare e condividere il progetto con l'amministrazione comunale ed ingaggiare tutti i soggetti pubblici e privati per creare un palinsesto di eventi. Cosa non di poco conto……
Quella che ci sembrava la parte più difficile è stata invece la più semplice. Abbiamo trovato un entusiasmo disarmante da parte di tutti, in primis da parte del Sindaco Orlando e di tutta l'amministrazione comunale;
Il nostro piccolo merito, se ne dobbiamo trovare uno, è stato quello di mettere tutti in relazione in un circolo virtuoso, per una causa nobile.
Il sogno finale è quello di avere un Parco "vivo", ricco di attività sociali ed economiche; un' area che possa offrire intrattenimento e opportunità di lavoro. Spero che un giorno, quando i miei figli diventeranno adulti, non ci sarà più solamente La Domenica Favorita ma ci saranno anche il Lunedi, il Martedi, il Mercoledi, il Giovedi, il Venerdi, il Sabato Favorita.

Chi vivrà vedrà…

L'autore: Marco Lampasona
È stato Direttore Generale del Dipartimento Studi Territoriali di Palermo, esperto del Ministro dello Sviluppo Economico, consulente della Presidenza del Consiglio e componente dell'Unità di Verifica degli Investimenti Pubblici. Ha maturato un expertise verticale in Business Management. Oggi è partner di innogea.

INNOGEA
Growing Healthcare

Innogea Srl
Sede Legale e operativa:
Via P.pe di Belmonte, 102 • 90139 Palermo
Tel. 091.7434774 • Fax 091.336853
Via Cadore, 6 • 20135 Milano
Tel. 02.83623040

www.innogea.com • info@innogea.com