PRIVACY E SICUREZZA A SUPPORTO DELL'INNOVAZIONE DIGITALE IN SANITÀ: IL NUOVO GDPR

A cura di

ASSOCIAZIONE ITALIANA
SISTEMI INFORMATIVI IN SANITÀ

In collaborazione con:

APiHM

ASSO DPO
Associazione Data Protection Officer

FIASO
Federazione Italiana Aziende Sanitarie e Ospedaliere

Clusit

PRIVACY E SICUREZZA A SUPPORTO DELL'INNOVAZIONE DIGITALE IN SANITÀ: IL NUOVO GDPR

Hanno contribuito alla stesura del documento

PARTECIPANTI AL GRUPPO DI LAVORO

Alzati Carlo - Medas - carlo.alzati@medas-solutions.it

Amato Andrea - AO San Gerardo Monza - andrea.amato@asst-monza.it

Armani Fiorella - DEDALUS - fiorella.armani@dedalus.eu

Arzarello Elisa - Intersystem - Elisa.Arzarello@intersystems.com

Bagnasco Manuela - ELCO - manuela.bagnasco@elco.it

Banorri Federica - ICT Regione Emilia - Federica.Banorri@regione.emilia-romagna.it

Barani Mauro - ASMN Reggio Emilia - Mauro.Barani@asmn.re.it

Barbetta Luca - Fujifilm - Luca.Barbetta@fujifilm.it

Bartolozzi Antonio - Medarchiver - bartolozzi@medarchiver.com

Beccari Fabio - IEO - fabio.beccari@ieo.it

Bertaina Fiorenzo - AO Cuneo - bertaina.f@ospedale.cuneo.it

Caccia Claudio - AISIS - presidenza@aisis.it

Chiarugi Cecilia - ICT Regione Toscana - cecilia.chiarugi@regione.toscana.it

Corrado Maurizio - Fiaso - corrado@fiaso.it.

D'Argenio Marzia - IBM - marzia_dargenio@it.ibm.com

De Luca Martina - ASL5 Friuli - martina.deluca@aas5.sanita.fvg.it

Ferrara Fabio - Studio Arnaboldi - fabio.ferrara@arnaboldi.eu

Ferri Sergio - AICA - sergioferri88@gmail.com

Fiora Sergio - ORACLE - sergio.fiora@oracle.com

Fouillouze Ornella - Club TI - ornella.fouillouze@gmail.com

Fregonara Medici Mario - AOU Novara - m.fregonaramedici@maggioreosp.novara.it

Genta Francesco - ELCO - francesco.genta@elco.it

Italiano Margherita - CSI Piemonte - margherita.italiano@csi.it

Intini Feliciano - Microsoft - feliciano.intini@microsoft.com

Jagher Veronica - Microsoft - vejagher@microsoft.com

Mangione Maurizio - FTGM - m.mangione@ftgm.it

Marrali Michele - Studio Storti - michele.marrali@studiostorti.com

Michieli Marco - AO Padova - marco.michieli@aopd.veneto.it

Miserendino Gandolfo - ICT Regione Emilia - gandomis@yahoo.it

Oliveri Agostino - GPI - agostino.oliveri@gpi.it

Picardi Riccardo - Engineering - Riccardo.Picardi@eng.it

Polito Filomena - AIPHIM - filopolito@libero.it

Polticchia Andrea - AGFA - andrea.polticchia@agfa.com

Ronchi Alberto - AISIS - a.ronchi@auxologico.it

Ronco Gian Luca - Emmonos - gianluca.ronco@emmonos.org

Sacco Luca - ELCO - luca.sacco@elco.it

Sala Piermauro - AO Santi Paolo e Carlo - piermauro.sala@asst-santipaolocarlo.it

Santoro Francesca - Deloitte - fsantoro@deloitte.it

Savoldi Matteo - Medas - matteo.savoldi@medas-solutions.it

Schena Elisa - INPECO - Elisa.Schena@inpeco.com

Scotti Paolo - INPECO - paolo.scotti@inpeco.com

Scuccimarra Micaela - Engineering - Micaela.Scuccimarra@eng.it

Simonelli Ettore - Engineering - esimonel@eng.it

Sini Elena - ICH - elena.sini@humanitas.it

Stefanelli Silvia - Studio Legale Stefanelli - s.stefanelli@studiolegalestefanelli.it

Stranieri Tommaso - Deloitte - tstranieri@DELOITTE.IT

Tabò Cinzia - USL1 Imperia - c.tabo@asl1.liguria.it

Telmon Claudio - CLUSIT - ctelmon@clusit.it

Vallega Alessandro - ORACLE - alessandro.vallega@oracle.com

Vaccaro Dario - Deloitte - davaccaro@deloitte.it

Veiluva Enzo - CSI Piemonte - enzo.veiluva@csi.it

Verroia Giulia - CSI Piemonte - giulia.verroia@csi.it

SOMMARIO

PREMESSA

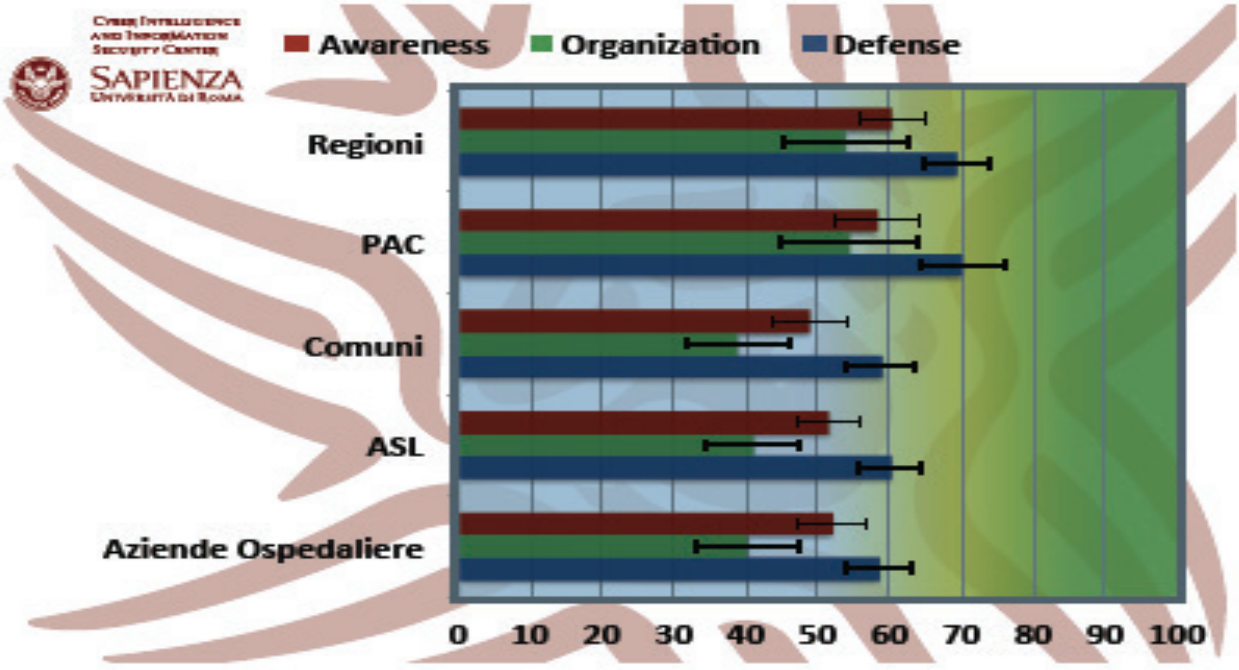
Il primo capitolo di questo documento è dedicato a una sintesi dei principali contenuti che verranno approfonditi nei successivi capitoli. Data la complessità dei temi trattati abbiamo ritenuto opportuno nel primo capitolo fornire una chiave sintetica di lettura del documento in modo da consentire un primo approccio "facilitato" permettendo un approfondimento successivo di tutti, o in parte, i capitoli del documento.

Il quadro che emerge dal rapporto sulla Sicurezza 2017 del Clusit[1] tende a confermare uno scenario di costante e quotidiano "allarme rosso" riguardo alle tematiche di cybersecurity nel settore della Sanità, che presume una tendenza generale ad un ulteriore peggioramento se il fenomeno non sarà contrastato con grande determinazione.
Ciò è inevitabile, a causa dell'aumento costante della superficie di attacco complessiva-mente esposta dalla nostra società digitale: si pensi non solo allo "smart working" sempre più diffuso, realizzato tramite un mix di strumenti mobile, cloud e social, spesso utilizzati in modo promiscuo ed insicuro (mescolando cioè senza criterio la vita digitale personale con quella lavorativa) ma anche alla diffusione impetuosa di device IoT, tipicamente privi delle più elementari misure di sicurezza, non più solo in ambito consumer ma anche in contesti produttivi oppure per applicazioni critiche, (per esempio in ambito e-health o smart-city).
A questi fenomeni corrisponde la crescente aggressività degli attaccanti, che ap-profittando delle numerose vulnerabilità del sistema (di natura culturale, organizzativa e tecnologica) conseguono profitti illeciti elevatissimi a fronte di rischi purtroppo ancora pra¬ticamente inesistenti, data la grande difficoltà oggettiva nel perseguire queste condotte con gli strumenti normativi e le risorse a disposizione, nonostante gli sforzi egregi delle autorità preposte.
Il Rapporto Clusit 2017 evidenzia che la Sanità, a livello internazionale, rappresenta il settore che ha subito il maggior incremento di attacchi informatici nel corso del 2016 rispetto al 2015 (+102%).

VITTIME PER TIPOLOGIA	2011	2012	2013	2014	2015	2016	Variazioni 2016 su 2015	Trend 2017
Institutions: Gov - Mil - LEAs - Intel	153	374	402	213	223	220	-1,35%	↘
Other targets	97	194	146	172	51	38	-25,49%	↓
Entertainment / News	76	175	147	77	138	131	-5,07%	↘
Online Services / Cloud	15	136	114	103	187	179	-4,28%	↘
Research - Education	26	104	70	54	82	55	-32,93%	↓
Banking / Finance	17	59	108	50	64	105	64,06%	↑
Software / Hardware Vendor	27	59	46	44	55	56	1,82%	↗
Telco	11	19	19	18	18	14	-22,22%	↓
Gov. Contractors / Consulting	18	15	2	13	8	7	-12,50%	↓
Security Industry	17	14	6	2	3	0	-100,00%	↓
Religion	0	14	7	7	5	6	20,00%	↑
Health	10	11	11	32	36	73	102,78%	↑
Chemical / Medical	2	9	1	5	2	0	-100,00%	↓
Critical Infrastructures	-	-	37	13	33	38	15,15%	↑
Automotive	-	-	17	3	5	4	-20,00%	↓
Org / ONG	-	-	19	47	46	13	-71,74%	↓
GDO / Retail	-	-	-	20	17	29	70,59%	↑
Hospitability	-	-	-	-	39	33	-15,38%	↘
Multiple targets (nuova)	-	-	-	-	-	49	-	-

1. Clusit, Rapporto sulla sicurezza ICT in Italia, 2017

Il Cyber Security Report 2014 dell'Università La Sapienza di Roma[2] ha evidenziato come, all'interno della PA, la Sanità sia un settore poco preparato ad affrontare il tema della sicurezza, sia nei suoi aspetti di consapevolezza sia in ragione alla pianificazione di soluzioni organizzative e tecnologiche. Inoltre la Sanità tende a essere uno dei settori della PA in cui è carente la propensione alla notifica delle Data Breach, mentre, trattandosi di sistemi complessi si presume che siano all'ordine del giorno non solo problemi di violazione dei dati, ma problemi relativi alla continuità operativa, al backup, all'utilizzo non autorizzato dei dati stessi. Da ultimo viene segnalato che due terzi del campione di Asl e Aziende Ospedaliere oggetto della survey, non effettuano attività di Risk Management.



L'adeguamento al GDPR (General Data Protection Regulation) Regolamento UE 2016/679 e alle linee guida AgID in merito alla misure minime di sicurezza ICT per la PA (Circolare n°1 del 17.3.2017 pubblicata in GU del 4.4.2017) costituisce quindi una concreta opportunità di migliorare la qualità e la sicurezza dei servizi ICT in Sanità, a tutela sia dei cittadini che utilizzano i servizi sociosanitari, sia dei professionisti che li erogano utilizzando ormai l'ICT come prerequisito delle ordinarie attività che vengono svolte nelle Aziende Sanitarie e Ospedaliere, sia infine degli stessi professionisti ICT che operano in Sanità, siano essi operatori delle Aziende Sanitarie o delle Aziende Fornitrici di soluzioni tecnologiche.

Allo scadere del mio secondo mandato come Presidente di Aisis, è un piacere invitarvi a leggere questo 6° documento di linee guida che Aisis ha prodotto in questi anni, rinnovando un ringraziamento a Alberto Ronchi, Cio del Gruppo Auxologico, per la sua preziosa attività di coordinamento del Gruppo di lavoro, e ai partecipanti al Gruppo che hanno prodotto questo interessante documento che, anche quest'anno, con grande piacere, AISIS presenta sperando di fornire indicazioni utili su un tema fortemente complesso.

Dott. Claudio Caccia, Presidente di Aisis
Torino, 12 ottobre 2017

2. Research Center of Cyber Intelligence and Information Security Sapienza Università di Roma, 2014 Italian Cyber Security Report, Dicembre 2014

1 —— Il GDPR in sintesi

1.1 —— Principi chiave

Il Regolamento UE n. 679/2016 sulla protezione dei dati personali (di seguito denominato GDPR) è entrato in vigore il 24 maggio 2016, e diverrà direttamente applicabile dal 25 maggio 2018 (termine ultimo di adeguamento), abrogando la Direttiva 95/46/CE.
Il GDPR rovescia completamente la prospettiva della disciplina sulla privacy, istituendo un quadro normativo incentrato sui doveri e la responsabilizzazione del Titolare del trattamento (principio di "accountability"). La nuova disciplina impone a tale soggetto di garantire il rispetto dei principi in essa contenuti, ma anche di essere in grado di comprovarlo, adottando una serie di strumenti che lo stesso GDPR indica, partendo da un'attenta valutazione di rischi e impatti, con una pianificazione fin da subito di una serie di attività che possono comportare modifiche culturali, organizzative e tecnologiche, nonchè significativi investimenti di natura economica.

Il concetto di "**responsabilizzazione**" si traduce nel fatto che il Titolare è chiamato a dimostrare che i trattamenti sono coerenti con il disposto del GDPR, a pianificare e mettere in atto misure tecniche e organizzative per poterne comprovare l'adeguatezza, e ad attivare un modello di monitoraggio delle misure tecnico-organizzative implementate.

In questa logica vengono introdotti due presupposti chiave dell'impianto del GDPR: la **Privacy by design**, quindi la necessità di disegnare le misure di Sicurezza e Privacy già in fase di progettazione dei sistemi informativi, e la **Privacy by default** vale a dire la capacità di disegnare le misure di Sicurezza e Privacy per default, come prerequisito di *normale funzionamento* dei sistemi informativi aziendali. (art. 25)

Inoltre vengono ribaditi i principi (art.5) di **liceità del trattamento** che può essere possibile solo se l'interessato ha espresso un esplicito consenso (che il Titolare deve dimostrare di aver raccolto, art.7), di **adeguatezza, pertinenza e non eccedenza dei dati** rispetto alle finalità per cui vengono trattati.

Successivamente alla enunciazione dei principi chiave, una attenzione particolare viene dedicata ai Diritti dell'interessato disciplinati in un apposito Capo del GDPR (Capo III):

- ***Informativa sul trattamento*** (art.12) laddove si evidenzia che deve essere fatta in forma concisa, trasparente, intellegibile e facilmente comprensibile e laddove si pone attenzione alla necessità di fornire precise indicazioni (art.13) sulla finalità del trattamento, gli eventuali destinatari/utilizzatori dei dati, il periodo di conservazione dei dati, le modalità per richiedere rettifica o cancellazione degli stessi
- ***Accesso*** ai dati da parte dell'interessato (art.15) che prevede al comma 3 la possibilità dell'interessato di ricevere copia dei dati trattati
- ***Rettifica e cancellazione dei dati***: diritto di rettifica (art.16), di cancellazione c.d. diritto all'oblio (art.17)

e di limitazione del trattamento (art.18) con obbligo di notifica all'interessato in caso di rettifica, cancellazione o limitazione (art.19)

- ***Portabilità dei dati***: l'interessato ha il diritto di ricevere in formato strutturato, di uso comune e leggibile da dispositivo automatico, i dati personali che lo riguardano e ha il diritto di trametter questi dati ad altro Titolare (art.20)
- **Diritto di opposizione**: diritto dell'interessato di opporsi al trattamento dei dati che lo riguardano in qualsiasi momento (art. 21) e diritto di non essere sottoposto a un processo decisionale automatizzato, compresa la profilazione (art.22)

1.2 —— Un possibile modello di riferimento

La complessità degli interventi da realizzare nell'area della innovazione digitale in Sanità richiede la valutazione, in fase di pianificazione (privacy by design) del sistema informativo aziendale, di due considerazioni di fondo:

- Non esiste il concetto di "sicurezza assoluta": qualsiasi sistema è vulnerabile. Mettere in sicurezza un sistema significa pianificare un insieme di procedure e strumenti che consentano di ridurre i rischi nella misura possibile o a livelli di accettabilità (Pfleeger, 2004, Cinotti, 2006)
- Gli interventi previsti sono di tipo **culturale**, **organizzativo**, **tecnologico** ed **economico**. Questi interventi in materia di innovazione digitale, sicurezza e privacy non costituiscono "limitazioni" a un utilizzo esteso e pervasivo di ICT in Sanità ma rappresentano azioni di qualificazione e di miglioramento del sistema informativo aziendale.

Un possibile modello di governance e di gestione delle azioni previste dal GDPR in Sanità viene rappresentata nel grafico seguente che tende a identificare cinque aree di attività che saranno trattate in modo maggiormente approfondito nei prossimi capitoli del documento.

1.3 —— Data inventory

L'obiettivo della prima area di attività è finalizzato alla conoscenza dei dati trattati. Si tratta di avere consapevolezza dei trattamenti attivi e quindi di conoscere per ogni tipologia di trattamento/dato trattato almeno le seguenti informazioni:

- Scopo del trattamento
- Descrizione dei dati d'uso
- Tipologia di dati trattati
- Le categorie dei destinatari (cui verranno comunicati i dati)
- Dov'è il database (collocazione nella server farm/in cloud etc)
- Limiti per la cancellazione/perdita dei dati
- Descrizione delle misure di sicurezza (organizzative e tecnologiche)
- Descrizione delle misure di backup e restore

Il GDPR prevede allo scopo la creazione di un "**registro dei trattamenti**" (art.30) che può essere redatto in forma scritta anche in formato elettronico (quindi digitale o cartacea).

Preso atto che con una certa frequenza nelle Aziende Sanitaria è difficilmente reperibile una mappa applicativa o un elenco di tutti gli applicativi, in logica di prima applicazione, appare sufficiente la redazione di un elenco (file xls) contenente le informazioni sopraindicate per singolo macro-processo aziendale supportato da ICT.

Registro dei Trattamenti								
Macroprocessi funzionali	Descrizione workflow processo	Scopo del trattamento	Tipologia e Descrizione Dato trattato	Descrizione db e sua allocazione	Possibili utilizzatori	Limiti per la cancellazione dei dati	Descrizione misure di sicurezza	Descrizione misure di backup
Anagrafe (MPI)	Gestione delle codifiche di base e Master Patient Index.							
Customer workflow management	Sperimentazione di un sistema di CWM che consente di tracciare il percorso del paziente in PS fornendo indicazioni anche agli accompagnatori. Necessaria analisi e revisione organizzativa dell'area accoglienza che appare frammentata. Processo attivo 24x7							
Prenotazione e Billing	Fase di prenotazione e pagamento in parte centralizzata e in parte decentrata in ambulatori o settori diagnostici. Dopo questa fase i pazienti vengono indirizzati direttamente agli ambulatori/reparti.Fase di accettazione in backoffice centralizzata dopo l'erogazione delle prestazioni prenotate.							
Accettazione e dimissione	Flusso standard di accettazione, trasferimento e dimissione. In parte centralizzato in parte decentrato nei reparti. Qualora il flusso venga totalmente decentrato nei reparti va considerato un processo 24x7							
Pronto Soccorso	Flusso standard di Triage, accesso alle sale visita, trasferimento in OBI e Medicina d'Urgenza.Necessità di perfezionare i passaggi tra Ps-Obi-MU. Necessità di verificare i flussi di integrazione con altri sistemi dell'area clinica. Criticita servizio 24x7							
Laboratorio Chimico Clinica	Flusso standard di Laboratorio con fase di order entry e recezione di referti e dati strutturati da reparto. Da attivare automazione microbiologia. Attivo laboratorio urgenza 24x7. Per gli esterni accettazione diretta con sistema Cup e predisposizione referti cartacea							
Laboratorio Micrologia	Flusso standard di Laboratorio di Virologia con fase di order entry e recezione di referti e dati strutturati da reparto. Da attivare automazione microbiologia. Attivo laboratorio urgenza 24x7. Per gli esterni accettazione diretta con sistema Cup e predisposizione referti cartacea							
Trasfusionale	Flusso standard di Laboratorio di Virologia con fase di order entry e recezione di referti e dati strutturati da reparto. Da attivare automazione microbiologia. Attivo laboratorio urgenza 24x7. Per gli esterni accettazione diretta con sistema Cup e predisposizione referti cartacea							
Anatomia Patologica	Classico flusso operativo di AP con fase di order entry e ricezione referti da reparto e soluzione cartacea per esterni.							
Imaging Radiologico	Flusso standard di gestione dell'imaging con order entry da reparto e consultazione di referti e immagini on line; esterni gestiti tramite cup e stampa dvd. Non attiva firma digitale. Sistema 24x7							
Blocco Operatorio	Flusso standard di gestione del blocco operatorio con rilevazione de tempi operatori e produzione del verbale di sala operatoria							
CCE di ricovero e ambulatoriale	Sistema che consnete di supportare il processo di ricovero attraverso la disponibilità di infromazioni cliniche on line							
Ciclo attivo, passivo e logistica	Processi dell'area amministativo contabile sostanzialmente in ordine con possibilità di miglioramenti favoriti dall'adozione del nuovo sistema Erp. Necessaria analisi sui flussi della logistica della farmacia.							
Gestione del personale	Processi dell'area Personale standard con livello di automazione solo per l'area presenze (no assenze) e stipendi. Le altre aree gestite manualmente.							
Document Management	Attivo un sistema di gestione documentale							
Protocollo e delibere	Attivo sistema di protocollo, gestione delle determine con relativo flusso autorizzativo.							
Dematerializzazione	Processo attualmente non presente. L'attivazione del sistema deve porre adeguate attenzioni sia sulle componenti organizzative e di governance (Reop. Conservazione) sia sulle componenti tecnologiche							
Direzionale	Attivo da anni sistema di programmazione e controllo di gestione. Non diffuse soluzioni di cruscottistica avanzata e/o di balancedscorecard							

Figura. Esempio non esaustivo di elenco dei trattamenti tipici di un'Azienda Sanitaria

1.4 ——— Analisi dei rischi e degli impatti

Preso atto dei dati trattati nei vari macro-processi aziendali, si pone, nella seconda area di attività da porre in essere, il problema di valutare i rischi connessi ai trattamenti e di una valutazione degli impatti connessi alla protezione dei dati.

Anche in questo caso in logica di prima applicazione (nel seguito del documento sono definiti approcci più articolati) si suggerisce la costruzione di una mappa dei rischi che consenta di stimare, per ogni tipologia di trattamento, un indice di rischio generico.

In tale contesto si suggerisce la costruzione di una matrice dei rischi che potrebbe essere articolata in:

- rischi esterni legati al fornitore della soluzione tecnologica
- rischi interni legati ai processi di trattamento del dato nel processo specifico
- rischi tecnologici legati alla sicurezza dell'infrastruttura tecnologica
- rischi di gestione legati all'organizzazione del team ICT aziendale

Per ogni tipologia di rischio vengono individuati degli item di verifica cui viene attribuito un punteggio di rischio. Questo consente di definire un rischio generico per singolo processo operativo supportato da ICT.

Successivamente può essere effettuata una valutazione degli impatti per singolo processo operativo supportato da ICT. A tale proposito si segnala che AgID ha prodotto una mappa che prevede tre tipologie di impatti: impatti organizzativi, impatti di servizio, impatti tecnologici. Anche in questo caso vengono definiti degli item di verifica per tipologia di impatto cui viene attribuito un punteggio. Questo consente di definire un indice di impatto per singolo processo operativo supportato da ICT. Nel caso specifico tuttavia, vanno tenuti in particolare considerazione gli impatti per i diritti e le libertà delle persone, non semplicemente riconducibili a impatti di servizio.

Struttura Impatti																
bassa 1, media 2, alta 3, critica 5	Macroprocesso	**Anagrafe (MPI)**	**Customer Workflow**	**Prenotazione e biling**	**ADT**	**PS**	**Lis**	**AP**	**Imaging**	**Blocco Oper**	**CCE ricovero e ambulatoriale**	**Ciclo attivo, paasivo**	**Personale**	**Document Management**	**Protocollo e Delibere**	**Direzionale**
Tipologia Impatto																
Impatti di servizio	Importanza del servizio a fini aziendali	4	3	4	2	3	4	3	3	4	4	3	3	2	2	3
	l'interruzione determina un immediato impatto/disagio agli utenti	4	4	4	3	4	4	3	4	4	4	2	2	2	2	2
	Tipologia e volume utenza coinvolta	4	3	4	4	3	4	3	4	3	4	2	2	2	2	1
	è possibile recuperare ex post i dati non acquisiti	4	1	4	1	2	3	2	2	2	3	2	2	1	1	1
	sono possibili procedure alternative	4	1	4	2	2	2	1	2	2	2	2	2	1	1	1
	livello di danno per l'Azienda	4	3	4	2	2	3	2	3	3	3	2	2	2	2	2
	Totale	***24***	***15***	***24***	***14***	***16***	***20***	***14***	***18***	***18***	***20***	***13***	***13***	***10***	***10***	***10***
Impatti organizzativi	numero UU.OO. coinvolte	3	2	3	4	2	4	3	4	4	4	3	3	2	2	2
	numero sedi coinvolte	3	2	3	2	1	4	2	4	4	4	1	1	2	2	2
	numerosità addetti coinvolti	3	2	3	1	2	4	3	4	4	4	2	2	2	2	1
	interruzione determina blocco del processo	4	1	4	1	3	3	2	2	3	3	3	3	2	2	2
	interruzine determina impatti su altri processi/sistemi interdipendenti	4	2	4	3	3	3	3	3	3	3	3	3	2	2	2
	Totale	***14***	***7***	***14***	***7***	***9***	***14***	***10***	***13***	***14***	***14***	***9***	***9***	***8***	***8***	***7***
Impatti Tecnologici	numero pdl coinvolte	3	2	3	3	2	3	2	3	3	4	2	2	2	2	1
	complessità architettura server	1	1	1	2	1	3	2	3	3	3	2	2	2	2	3
	complessità architettura applicativa	3	1	3	1	1	3	2	3	3	3	2	2	2	2	3
	Interruzione servizi applicativi, Interruzione sistema di integrazione, anomalie database	3	2	3	3	3	3	2	3	3	3	2	2	2	2	2
	Dimensione db	3	1	3	2	1	3	1	4	3	3	2	2	2	2	2
	Tempo restore/reinstallazione applicativo	3	2	3	2	2	3	2	2	2	3	2	2	2	2	3
	Tempo restore db	3	2	3	2	2	2	2	3	2	2	2	2	2	2	3
	Totale	***19***	***11***	***19***	***15***	***12***	***20***	***13***	***21***	***19***	***21***	***14***	***14***	***14***	***14***	***17***

Figura. Esempio non esaustivo di elenco dei trattamenti tipici di un'Azienda Sanitaria

La sommatoria dell'indice di rischio e dell'indice di impatto determinano un indice di Gravità per singolo processo operativo supportato da ICT.

L'indice di Gravità moltiplicato per un indice di probabilità di accadimento dell'evento correlato alle misu-

re già adottate) e un indice di vulnerabilità (tipico della complessità del processo specifico) determina un **indice di Rischio reale** per singolo processo operativo supportato da ICT, valutato complessivamente nei suoi aspetti di rischio generico, di impatti di probabilità e vulnerabilità.[3]
Questo tipo di approccio consente peraltro di utilizzare i risultati ottenuti anche per il Piano di Bussiness Continuity coerenetemente con le indicazioni di AgID.

1.5 —— Misure organizzative

L'obiettivo delle attività di tale area consistono nella verifica principalmente di:

- Definizione Organigramma Privacy
- Nomina Data Protection Officer
- Definizione Titolarietà/Co-Titolarietà (Pdta)
- Nomina Responsabili dei trattamenti
- Nomina degli Autorizzati al trattamento (già Incaricati ex Dl.Lgs.196/2003) alla luce della Raccomandazione espressa dall'Autorità Garante
- Gestione documentale degli interventi di Sicurezza e Privacy (documentazione Organizzativa e Tecnica)
- Notifica dei Data Breach

Non si rilevano particolari segnalazioni in merito alla definizione dell'organigramma della privacy, tendenzialmente sovrapponibile a quella del D.Lgs 196/03, e conseguentemente alla nomina del Titolare, dei Responsabili e, ancorché non espressamente previsto dal GDPR, degli Autorizzati al trattamento dati personali per conto del Titolare o dei Responsabili. In questo ultimo caso, il Garante privacy ha espresso l'opportunità che titolari e responsabili del trattamento mantengano in essere la struttura organizzativa e le modalità di designazione degli incaricati di trattamento così come delineatesi negli anni anche attraverso gli interventi del Garante stesso.[4] In tale contesto, altresì, si segnala l'opportunità, presente nell'art.28 comma 6, di utilizzare "contratti tipo" per le nomine del personale autorizzato al trattamento qualora svolga attività omogenee (ad es. gli Os/Ota, il personale infermieristico, il personale medico…) semplificando la gestione documentale della privacy.

Il tema della **Co-titolarietà dei dati** (art.26) è un tema particolarmente interessante in Sanità in quanto semplifica il quadro normativo rispetto a trattamenti che possono esser svolti da più titolari su uno specifico processo di cura. Ci si riferisce prevalentemente al tema dell'utilizzo di nuovi modelli organizzativi, di tipo trasversale (ospedale-territorio-domicilio), denominati PDTA, per il trattamento della cronicità. Con frequenza questi nuovi modelli organizzativi comportano un trattamento svolto da più professionisti in luoghi e tempi

3. In letteratura il Rischio (R) corrisponde a R = Impatto * Probabilità (di accadimento) e la valutazione dell'impatto dipende dalle minacce e dalla vulnerabilità, vedi ad es. Linee guida per l'analisi del Rischio, Clusit, 2012
4. Raccomandazione del Garante privacy: http://www.garanteprivacy.it/Titolare-responsabile-incaricato-del-trattamento

diversi ma anche appartenenti a legal entity diverse. Il GDPR prevede la possibilità di contrattualizzare la cotitolarietà, definendo le reciproche responsabilità e dandone chiara e trasparente informazione ai cittadini (come normato agli art.13 e 14).
Un secondo tema interessante riguarda la **nomina e il ruolo del DPO** (art. 37,38, 39). Il DPO è una nuova figura che deve avere conoscenza specifica della normativa (su privacy e sicurezza) e della prassi in materia di protezione dei dati. Si segnala in proposito, pur se al momento non è un requisito obbligatorio, l'esistenza di specifici percorsi formativi e di percorsi di certificazione delle competenze del DPO.
Può essere un dipendente o un consulente/società esterna. Deve esser coinvolto in tutte le attività riguardanti la protezione dei dati. Svolge compiti di consulenza al Titolare e ai Responsabili del trattamento, sorveglia l'osservanza delle attività poste in essere per l'adeguamento al GDPR, fornisce parere all'Autorità di controllo, rappresentando il punto di contatto tra quest'ultima e l'Azienda di riferimento.

Un terzo tema di interesse è la notifica obbligatoria del data breach. La notifica, in caso di violazione dei dati personali, è obbligatoria entro 72 ore all'Autorità Garante (art. 33) ma altresì obbligatoria (art. 34) nei confronti dell'interessato.

L'ultimo tema di un certo interesse anche per la Sanità è la creazione (o l'utilizzo se esistente) di un sistema di gestione documentale per tutta la documentazione prodotta sulla protezione dei dati a fini di esibizione a terzi tesa a dimostrare in modo oggettivo e trasparente le attività poste in essere per la compliance al GDPR, in linea con il principio di accountability.

1.6 —— Misure tecnologiche

Trattasi di attuare e descrivere le misure tecnologiche poste in essere al fine di garantire un livello di rischio adeguato relativamente ai diritti e alle libertà delle persone fisiche derivanti dai trattamenti effettuati, compresi quelli relativi alla riservatezza, integrità e disponibilità dei dati (art. 32) per ogni processo operativo supportato da ICT. Si suggerisce in proposito di adottare un approccio globale (multidimensionale) e sistemico considerando che ci si riferisce in particolare a quattro aree di attività che impattano sui processi di business e richiedono interventi Culturali, Organizzativi, Tecnologici, Economici.

In particolare si fa riferimento alla gestione unificata dell'identità e dei profili di accesso degli utilizzatori dei dati (IAM) e del tracciamento delle loro attività, la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; la capacità di rilevare eventi ed incidenti, riconducibile al tema della gestione dei data breach, la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; la messa in opera di una procedura/sistema per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

1.7 —— Misure applicative

Tra le misure applicative da porre in essere, particolare attenzione deve essere dedicata:

- all'integrazione dei sistemi applicativi con il sistema di gestione delle identità e dei profili di accesso di cui al punto precedente
- alla pseudonimizzazione e alla cifratura dei dati personali (art. 32)
- alla gestione unificata dell'informativa, consensi, rettifica e cancellazione (art da 7 a 10 e da 15 a 19). In merito a quest'ultimo punto l'analisi della mappa applicativa deve consentire di precisare quali procedure acquisiscono il consenso/limitazioni del cittadino e come rendono trasparente questo attributo a tutti gli applicativi coinvolti nel singolo processo di cura al fine di garantire che i dati personali siano consultati solo dal personale effettivamente coinvolto in uno specifico processo di cura e solo per la durata del processo di cura.

1.8 —— Misure minime di sicurezza AgID

Tra le misure tecnologiche da porre in essere non possono essere tralasciate le indicazioni AgID in merito alle misure minime di sicurezza ICT per la Pubblica Amministrazione[5], che devono essere adottate al fine di contrastare le minacce più comuni.

AgID, facendo riferimento al modello CIS Critical Security Controls for Effective Cyber Defense predisposto da Sans Istitute nel 2015, ha creato un set di controlli di verifica sulle prime 5 aree di rischio previste dal modello Sans-20 (le aree del modello sono per l'appunto 20) che, a parere non solo di AgID, rappresentano l'insieme dei controlli indispensabili per assicurare il minimo livello di protezione nella maggior parte delle situazioni.

Tali controlli, definiti con l'acronimo ABSC (AgID Basic Security Control) riguardano le seguenti aree:

ABSC1 inventario dei dispositivi autorizzati e non autorizzati presenti in rete tramite discovery dei dispositivi, implementare il logging dei DHCP, gestire l'inventario delle risorse in rete registrando almeno l'IP, installare autenticazione a livello di rete per limitare i dispositivi che possono essere connessi in rete

ABSC2 inventario dei software autorizzati e non autorizzati presenti in rete mediante strumenti automatici di inventory non consentendo l'installazione di altri software esclusi da questo elenco, implementare una whitelist dei sw autorizzati bloccando l'esecuzione dei sw non inclusi nella whitelist, gestire l'inventario del sw

ABSC3 proteggere configurazioni hw e sw sui dispositivi mobili, laptot, workstation e server

Definire e programmare configurazioni standard per ws, server e altri tipi di sistemi, assicurare con regolarità la validazione e l'aggiornamento delle immagini d'installazione che devono essere conservate in modalità protetta, eseguire le operazioni di amministrazione su tutte le tipologie di macchine per mezzo di connessioni protette, utilizzare strumenti possibilmente automatici per verificare l'integrità dei file critici di sistema monitorando che non vengano alterati

5. AgID, Misure minime di sicurezza ICT per le pubbliche amministrazioni, Gazzetta Ufficiale 79 del 4 aprile 2017 n°79 - Circolare 17.3 2017 n°2/2017 www.gazzettaufficiale.it/eli/id/2017/04/04/17A02399/sg

ABSC4 valutazione e correzione continua della vulnerabilità

Usare uno SCAP (Security Content Automation Protocol) per esguire la validazione di vulnerabilità, verificare che gli strumenti di scansione delle vulnerabilità siano utilizzati periodicamente, registrarsi a un sistema che fornisca tempestivamente le informazioni su nuove minacce e vulnerabilità

ABSC5 uso appropriato dei privilegi di amministratore

Limitare i privilegi di amministratore ai soli utenti che abbiano adeguate competenze, assegnare le utenze di amministratore solo con i privilegi necessari per svolgere attività specifiche, logging delle azioni compiute dagli amministratori, mantenere l'inventario delle utenze di amministratore con warning ogni volta venga aggiunta una nuova utenza, tracciare nei log i tentativi falliti di creazione di nuove utenze di amministratore, conservare le credenziali in modo da garantirne disponibilità e riservatezza

In aggiunta ai primi 5 set di controlli sono elencati, in GU, anche i seguenti controlli:

ABSC8 difese contro i malware

Installare su tutti i sistemi connessi in rete soluzioni antivirus con archiviazione centrale degli eventi rilevati, installare firewall e IPS personali, limitare luso di dispositivi esterni a quelli necessari allo svolgimento delle attività aziendali e monitorare i tentativi di utilizzo di dispositivi esterni, utilizzo di sistemi di content filtering e antisapamming,

ABSC10 Copie di sicurezza

Effettuare almeno settimanalmente backup che deve riguardare sitema operativo, applicativi e database, verificare periodicamente le funzioni e i risultati delle procedure di restore, effettuare backup multipli per avere certezza di disponibilità di almeno una copia di backup, assicurarsi che almeno una copia del backup non sia permanentemente accessibile dal sistema.

1.9 —— Il regime sanzionatorio

Solo poche righe per ricordare che il trattamento illecito dei dati o la perdita di dati prevede sia **responsabilità di natura penale** per la mancata adozione di misure minime di sicurezza, sia **responsabilità di natura civile** in quanto l'omissione di misure idonee determina un obbligo risarcitorio di cui all'art.2050 del Codice Civile e ai sensi dell'art.15.del D.Lgs.196/03 sia **responsabilità di tipo amministrativo**.
In merito a quest'ultime, il nuovo GDPR (art.83) prevede sanzioni amministrative pecuniarie **fino a 10 milioni di euro e per le imprese pari al 2% del fatturato di gruppo mondiale** in caso di violazione degli obblighi del Titolare del trattamento (art. 8,11 da 25 a 39, 42, 43) e **fino a 20 milioni di euro e per le imprese pari al 4% del fatturato di gruppo mondiale** in caso di violazione delle condizioni relative al consenso (art. 5,6,7,9) al rispetto dei diritti dell'interessato (art. da 12 a 22) e dei trasferimenti dati da un Titolare all'altro di Paesi terzi (art.da 44 a 49).

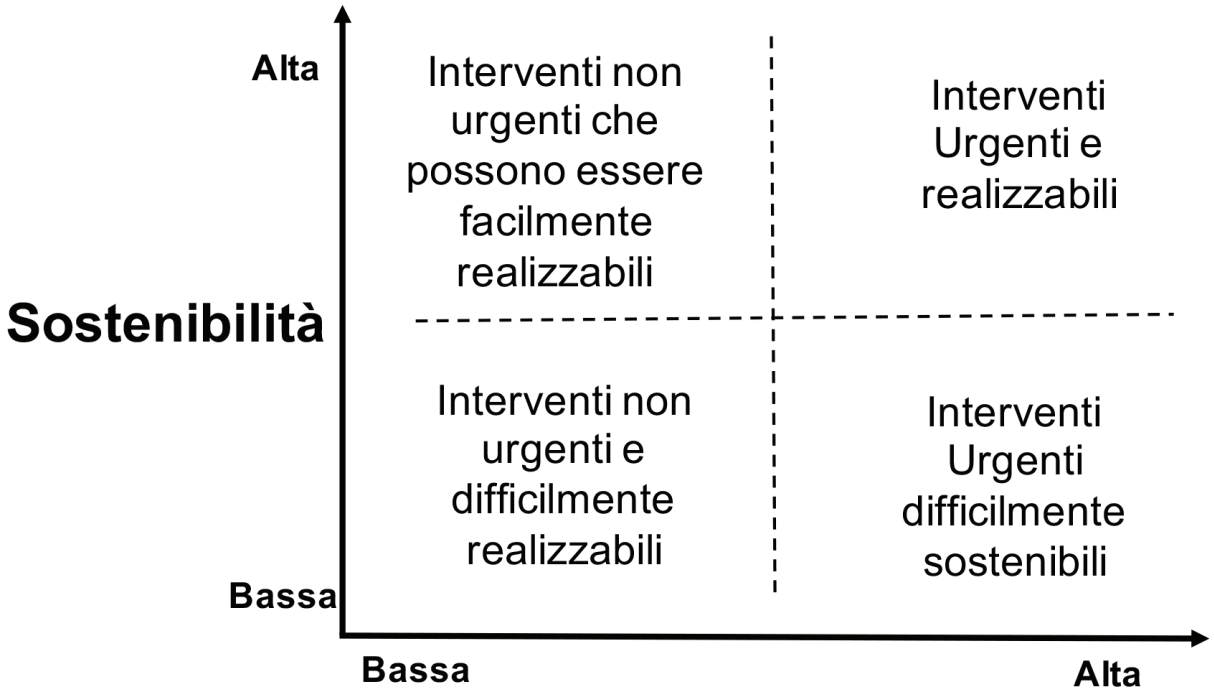
1.10 ——— Cosa fare: un possibile modello di azione

Dalle analisi e valutazioni effettuate relativamente alla possibile attivazione delle misure trattate nel secondo capitolo, appare necessario effettuare una valutazione della reale sostenibilità delle stesse e dei tempi in cui tali misure possono essere realizzate.

In proposito si ipotizza l'utilizzo di una matrice in cui le varie misure vengono posizionate in termini di **sostenibilità** e di **priorità**.

La sostenibilità è rappresentata dalla valutazione di variabili come costi di realizzazione, livelli di impatto sull'organizzazione e sull'impianto tecnologico aziendale, velocità di implementazione, semplicità degli interventi da adottare.

La priorità è sostanzialmente determinata dal livello esistente del Gap tra As Is e To Be (maggiore è il gap maggiore è la priorità) e dai livelli di mitigazione dei rischi/impatti (anche in questo caso maggiore è il livello di rischio, maggiore e la probabilità)



L'utilizzo della matrice rende possibile la collocazione delle misure di sicurezza/privacy da adottare in quattro quadranti che possono dare indicazioni rispetto alle attività da porre in essere in logica di reale sostenibilità e priorità.

Preso atto che in Sanità il problema delle risorse economiche dedicate all'ICT è particolarmente critico, sarà più facile porre attenzione, almeno in una fase inziale, agli interventi che si posizionano nei due quadranti superiori, che possono essere facilmente realizzati, lasciando a una seconda fase la realizzazione degli interventi collocati nella parte bassa della matrice che probabilmente sono meno sostenibili dal punto di vista economico o di complessità.

Al fine di facilitare un primo self assesment sui temi di Sicurezza e Privacy, Aisis ha predisposto un modello "Privacy Assessment Tool - Health", che consente un posizionamento su un grafico a radar della compliance del sistema informativo di un'azienda sanitaria rispetto sia al GDPR, sia ai requisiti minimi di sicurezza di AgID, con l'obiettivo di consentire una rapida consapevolezza della compliance e di stimolare un piano di azioni condivise con la Direzione strategica.

Il tool, basato su un file xls, verrà reso disponibile sul sito Aisis tra la documentazione del convegno 2017.

2 ——— GDPR: novità, ambiti di applicazione e sanzioni

2.1 ——— Le novità del GDPR

Il Regolamento europeo 2016/679 ribadisce e conferma elementi già conosciuti nell'attuale ordinamento italiano sulla protezione dei dati personali, ma introduce svariate novità al fine di poter garantire un alto livello di tutela degli interessati con un approccio ed una metodologia incentrati sulla sempre maggiore responsabilizzazione dei soggetti che trattano i dati, vale a dire il Titolare e il Responsabile, anche se gli stessi non fossero stabiliti nell'Unione Europea. La condizione sufficiente è quella di trattare i dati di interessati che si trovano nell'Unione quando le attività di trattamento riguardano la prestazione dei servizi/beni agli stessi o riguardano il monitoraggio del comportamento degli stessi.
Di seguito verranno sinteticamente illustrate le principali novità del GDPR.

Anzitutto il Regolamento introduce il nuovo principio di responsabilizzazione (accountability) che costituisce il punto centrale della normativa in materia di protezione dei dati personali. Secondo tale principio, il Titolare è obbligato a mettere in atto entro il 25 maggio 2018, e successivamente in modo costante, "misure tecniche e organizzative adeguate" che devono essere costantemente, verificate, monitorate ed aggiornate, ove necessario, "per garantire, ed essere in grado di dimostrare" che il trattamento è sempre effettuato in modalità conforme al Regolamento.
Il Regolamento introduce ed amplifica anche i concetti di protezione dei dati fin dalla progettazione (Privacy by Design) e per impostazione predefinita (Privacy by Default), secondo cui il Titolare deve predisporre e mettere in atto delle misure tecniche ed organizzative per attuare i principi di protezione dei dati integrando nel trattamento tutte le necessarie garanzie, concetti peraltro già presenti nel codice privacy italiano.
Risultano accresciuti ed estesi i diritti degli interessati che con il Regolamento includono il nuovo "diritto alla portabilità dei dati" ed il "diritto all'oblio" (in precedenza era riconosciuto solo a livello giurisprudenziale), oltre al diritto di essere informato con modalità semplici e trasparenti e con linguaggio chiaro e facilmente comprensibili, il diritto di accesso, il diritto di rettifica, la limitazione del trattamento, il diritto di opposizione, il diritto di non essere sottoposto ad un processo decisionale automatizzato (profilazione), il diritto di essere informato della rettifica o cancellazione dei dati, il diritto al risarcimento del danno materiale o immateriale, ove venga ad occorrere.
Viene introdotta la nuova figura del Responsabile della protezione dei dati (Data Protection Officer o RPD), da non confondere con il responsabile del trattamento. Trattasi di una figura che dovrà essere obbligatoriamente designata in caso di trattamento effettuato da un'Autorità pubblica o un organismo pubblico, o se il Titolare o il Responsabile effettuano un trattamento che richiede un monitoraggio su larga scala, oppure se vengono effettuati trattamenti su larga scala di categorie particolari di dati o dati relativi a condanne penali o reati.
Viene introdotto per il Titolare ed il Responsabile del trattamento il nuovo obbligo di tenere un registro in forma scritta, anche in formato elettronico, delle attività di trattamento svolte che contiene le informazioni ed i documenti prescritti dal Regolamento.

Si ribadisce l'obbligo di istruire il Responsabile del trattamento o chiunque agisca sotto la sua autorità o sotto quella del Titolare (questa figura riscontra quello che la legislazione italiana individua come '"incaricato" del trattamento ai sensi dell'art.30 del Dl.Lgs.196/2003).

Le persone deputate al trattamento dei dati personali (che corrispondono agli attuali "incaricati") devono essere autorizzate espressamente (per iscritto) ed istruite in modalità dimostrabile.

L'informativa (attuale ex. Art.13 del Dl.Lgs. 196/2003) da rendere all'interessato deve essere concisa, trasparente, intellegibile e facilmente accessibile. Ma il punto focale è che deve essere resa con un linguaggio semplice e chiaro, anche in combinazione con icone standardizzate. Il Regolamento, inoltre, demanda alla Commissione Europea la facoltà ed il potere di adottare atti delegati per stabilire le informazioni da presentare sotto forma di icona e le procedure atte a fornire le icone standardizzate.

Devono poi essere rispettate le condizioni per il rilascio di un valido consenso da parte dei minori di 16 anni.

Le misure di sicurezza ed organizzative adottate devono essere dimostrabili e devono garantire un livello di sicurezza adeguato al rischio.

Qualsiasi violazione di dati personali (c.d. data breach) deve essere notificata al Garante e, in presenza di determinati presupposti, anche agli interessati entro il termine di non oltre 72 ore. Viene invece eliminato in toto l'obbligo di notificazione preventiva previsto attualmente dall'art. 37, D.Lgs. 196/2003.

L'approccio al trattamento deve essere basato sul rischio ed è mandatorio effettuare una valutazione di impatto sulla protezione dei dati e procedere a consultazione preventiva presso l'autorità di controllo se la valutazione di impatto evidenzia un rischio elevato in assenza di misure per attenuare il rischio, o nel caso quelle che dovrebbero essere implementate siano troppo onerose/sproporzionate per le capacità del Titolare.

Viene introdotta l'adozione di codici di condotta e di meccanismi di certificazione quale ausilio al Titolare e al Responsabile per dimostrare la conformità alle disposizioni del Regolamento.

Sono attribuiti maggiori è più vasti poteri alle autorità di controllo nazionali, definiti i compiti e poteri dell'autorità di controllo capofila in caso di trattamenti transfrontalieri, istituito il Comitato Europeo per la protezione dei dati.

L'impianto sanzionatorio diventa particolarmente severo ed equivalente in tutti gli Stati membri. Le sanzioni amministrative pecuniarie, che devono essere effettive, proporzionate e dissuasive in relazione al singolo caso, possono arrivare fino a euro 20 milioni, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore. Gli Stati membri hanno facoltà di stabilire, inoltre, norme relative ad altre sanzioni. (in Germania il recepimento del GDPR gia approvato prevede come già nel nostro ordinamento attuale pesanti sanzioni penali)[6]. Per quello che riguarda l'Italia, al momento in cui si è redatto il presente documento, siamo in attesa della legge "Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea - Legge di delegazione europea 2016 - 2017" in questo momento con DDL 2834 approvata dal SENATO in data 2 agosto 2017 e trasmesso alla Camera in data 3 agosto 2017.[7]

Per quanto ci è dato di sapere al momento, e riprendendo il testo del DDL 2834, dall'art.13 che riportiamo testualmente:

6. www.bmi.bund.de/SharedDocs/Downloads/EN/Gesetzestexte/datenschutzanpassungsumsetzungsgesetz.pdf?__blob=publicationFile

7. www.senato.it/japp/bgt/showdoc/frame.jsp?tipodoc=Emendc&leg=17&id=1029112&idoggetto=1035671 omissis - (Delega al Governo per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE)

1. Il Governo è delegato ad adottare, entro sei mesi dalla data di entrata in vigore della presente legge, con le procedure di cui all'articolo 31 della legge 24 dicembre 2012, n. 234, acquisiti i pareri delle competenti Commissioni parlamentari e del Garante per la protezione dei dati personali, uno o più decreti legislativi al fine di adeguare il quadro normativo nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.
2. I decreti legislativi di cui al comma 1 sono adottati su proposta del Presidente del Consiglio dei ministri e del Ministro della giustizia, di concerto con i Ministri degli affari esteri e della cooperazione internazionale, dell'economia e delle finanze, dello sviluppo economico e per la semplificazione e la pubblica amministrazione.
3. Nell'esercizio della delega di cui al comma 1 il Governo è tenuto a seguire, oltre ai princìpi e criteri direttivi generali di cui all'articolo 32 della legge 24 dicembre 2012, n. 234, anche i seguenti princìpi e criteri direttivi specifici:

   a) abrogare espressamente le disposizioni del codice in materia di trattamento dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196, incompatibili con le disposizioni contenute nel regolamento (UE) 2016/679;

   b) modificare il codice di cui al decreto legislativo 30 giugno 2003, n. 196, limitatamente a quanto necessario per dare attuazione alle disposizioni non direttamente applicabili contenute nel regolamento (UE) 2016/679;

   c) coordinare le disposizioni vigenti in materia di protezione dei dati personali con le disposizioni recate dal regolamento (UE) 2016/679;

   d) prevedere, ove opportuno, il ricorso a specifici provvedimenti attuativi e integrativi adottati dal Garante per la protezione dei dati personali nell'ambito e per le finalità previsti dal regolamento (UE) 2016/679;

   e) adeguare, nell'ambito delle modifiche al codice di cui al decreto legislativo 30 giugno 2003, n. 196, il sistema sanzionatorio penale e amministrativo vigente alle disposizioni del regolamento (UE) 2016/679 con previsione di sanzioni penali e amministrative efficaci, dissuasive e proporzionate alla gravità della violazione delle disposizioni stesse. - omissis -

   si rileva che la posizione del legislatore sia quella, è evidente, di adeguare il sistema sanzionatorio penale vigente al disposto del GDPR, con la previsione di sanzioni, anche **penali, efficaci, proporzionali e dissuasive.**[8]

2.2 —— L'ambito di applicazione del regolamento

Il Regolamento UE 2016/679 ha come oggetto la protezione delle persone fisiche relativamente al trattamento dei dati personali e la libera circolazione dei dati nell'Unione Europea che non può essere limitata né vietata.

L'art. 4, par. 1, del Regolamento definisce il "dato personale" come "qualsiasi informazione riguardante una

8. www.senato.it/japp/bgt/showdoc/17/DDLMESS/1040253/index.html

persona fisica identificata o identificabile", ivi inclusi i dati personali sottoposti a tecniche di pseudonimizzazione[9]. I dati anonimi restano invece esclusi in toto dall'ambito di applicazione del Regolamento.
La definizione di "dato personale" corrisponde in pieno a quanto definito in precedenza nel contenuto nella Direttiva 95/46/CE da cui deriva la vigente normativa nazionale in materia di protezione dei dati personali applicabile fino al 24 maggio 2018 e, pertanto, dà piena conferma della volontà del legislatore europeo di avere una nozione ampia di dato personale ed assolutamente non vincolata dall'evoluzione tecnologica.
Relativamente al "trattamento", lo stesso è definito dall'art. 4, par. 2, del Regolamento come "qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione".
Anche la definizione di "trattamento" riproduce in sostanza quanto già definito nei contenuti della Direttiva 95/46/CE, includendo nelle esemplificazioni delle operazioni di trattamento la "strutturazione" e la "limitazione", mentre è stato soppresso il "blocco" dei dati (ora presente nella esplicitazione del concetto di trattamento).

2.2.1 ——— L'ambito di applicazione materiale

Il Regolamento 679/2016 si applica a qualsiasi trattamento di dati personali contenuti in un archivio o destinati a figurarvi, in modo indipendente dal fatto che si tratti di un trattamento interamente o parzialmente automatizzato, ovvero non automatizzato, intendendosi per "archivio" "qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico".

Pertanto, come chiarito dal Considerando n. 15 del GDPR, non dovrebbero rientrare nell'ambito di applicazione del Regolamento "i fascicoli" o "la serie di fascicoli" non strutturati secondo criteri specifici.

Per espressa previsione dell'art. 2, par. 2, il Regolamento non si applica ai trattamenti di dati personali:

a) effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione europea;
b) effettuati dagli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione del titolo V, capo 2, TUE ;
c) effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico;

9. «pseudonimizzazione»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile
10. "DISPOSIZIONI SPECIFICHE SULLA POLITICA ESTERA E DI SICUREZZA COMUNE"
11. Il Regolamento 45/2001 dovrà essere adeguato ai principi e alle norme del Regolamento 2016/679 in conformità all'art. 98 del Regolamento 2016/679, restando altresì impregiudicata l'applicazione della direttiva 2000/31/CE e in particolare le norme relative alla responsabilità dei prestatori intermediari di servizi di cui agli articoli da 12 a 15 della medesima direttiva.

d) effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse.

Il trattamento dei dati personali da parte di istituzioni, organi, uffici e agenzie dell'Unione Europea è invece soggetto alle disposizioni del Regolamento (CE) n. 45/2001.

2.2.2 —— L'ambito di applicazione territoriale

Ai sensi dell'art. 3, il Regolamento si applica ai Titolari ed ai Responsabili del trattamento stabiliti in uno Stato dell'Unione Europea, ovvero in un luogo soggetto al diritto di uno Stato membro, indipendentemente dal fatto che il trattamento sia o meno effettuato nell'Unione qualora comunque rientrasse nell'ambito delle attività di uno stabilimento di un Titolare o responsabile nell'Unione.
Il Regolamento si applica, inoltre, ai Titolari o Responsabili non stabiliti nell'Unione Europea se trattano i dati personali di interessati che si trovano nell'Unione Europea, quando le attività di trattamento riguardano nello specifico:
a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato;
b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione.

2.3 —— Le sanzioni

Il Regolamento UE 2016/679 fissa all'articolo 83 il tetto massimo di ammende pecuniarie di tipo amministrativo, lasciando alle singole Autorità competenti un ampio potere discrezionale in merito al valore economico della singola sanzione; per gli illeciti penali, i singoli Stati membri hanno la facoltà di emettere disposizioni relative alle sanzioni penali per violazioni della normativa (vedi par.2.2).
Le sanzioni si applicano agli attori del trattamento (Titolari del trattamento e Responsabili del trattamento) e agli organismi accreditati e deputati al controllo o al monitoraggio dei Codici di Condotta e al rilascio delle certificazioni.
Le sanzioni amministrative pecuniarie possono essere somministrate:
fino a un valore massimo di 10.000.000 € o, per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, per le tipologie di violazioni di seguito illustrate, per ciascuna delle quali si riportano i relativi articoli della norma di riferimento:

- obblighi del Titolare e del Responsabile del trattamento (artt. 8, 11, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 42 e 43);
- obblighi dell'organismo di certificazione (artt. 42 e 43);
- obblighi dell'organismo di controllo (art. 41 comma 4).

fino a un valore massimo di 20.000.000 € o, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, per le tipologie di violazioni di seguito illustrate, per ciascuna delle quali si riportano i relativi articoli della norma di riferimento:

- i principi di base del trattamento, comprese le condizioni relative al consenso (artt. 5, 6, 7 e 9);

- i diritti degli interessati (artt. da 12 a 22);
- i trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale (artt. da 44 a 49);
- gli obblighi ai sensi delle legislazioni degli Stati membri (artt. da 85 a 91);
- inosservanza di ordini o limitazioni da parte dell'Autorità di Controllo o negato accesso (artt. 58 paragrafo 1 e 2).

Se lo stesso trattamento o più trattamenti collegati avvengono per dolo o colpa grave con violazioni a più di una disposizione della normativa, l'importo totale della sanzione amministrativa pecuniaria non supera l'importo specificato per la violazione più grave.

I poteri sanzionatori dell'Autorità competente sono soggetti a garanzie procedurali adeguate in conformità del diritto dell'Unione e degli Stati membri, inclusi il ricorso giurisdizionale effettivo e il giusto processo.

L'Autorità competente, alla quale è assegnato un ampio potere discrezionale, determinerà caso per caso l'ammontare della sanzione comminabile, valutando:

- natura, gravità e durata della violazione, numero d'interessati e portata del danno subito;
- carattere doloso o colposo della violazione;
- le misure adottate per attenuare il danno subito dagli interessati;
- il grado di responsabilità alla luce delle misure tecniche ed organizzative adottate ai sensi degli articoli 25 (Privacy by design e by default) e 32 (Sicurezza del trattamento);
- eventuali precedenti violazioni pertinenti riscontrate e rispetto degli eventuali provvedimenti emessi in merito dall'Autorità;
- il grado di cooperazione con l'Autorità nel porre rimedio alla violazione e attenuare i suoi effetti;
- le categorie di dati personali interessate dalla violazione;
- la modalità con la quale l'Autorità di controllo è stata informata della violazione;
- l'eventuale adesione a codici di condotta approvati ai sensi dell'articolo 40 o a meccanismi di certificazione approvati ai sensi dell'articolo 42;
- la valutazione di possibili benefici economici «abilitati» dalla violazione (benefici finanziari conseguiti o perdite evitate, direttamente o indirettamente, in conseguenza della violazione).

3 —— Data Inventory

3.1 —— Tipologia di dati trattati

Per **dato personale** s'intende "qualsiasi informazione riguardante una persona fisica identificata o identificabile: si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale".

In relazione alla tipologia di informazioni da essi veicolate, alcuni dati personali sono inseriti dal Regolamento UE 2016/679 in apposite categorie. All'eventuale violazione di questi dati "particolari" è associato un rischio maggiore per i diritti e le libertà fondamentali degli individui a cui le informazioni si riferiscono; il trattamento dei dati personali appartenenti a queste "categorie particolari" necessita perciò di maggiori cautele e garanzie.

Si tratta di tutti i dati atti a rivelare l'origine razziale o etnica, le opinioni politiche, l'appartenenza sindacale e le convinzioni religiose o filosofiche di un individuo, insieme alle informazioni genetiche, ai dati biometrici, alle notizie in merito alla salute, alla vita o all'orientamento sessuale della persona (**articolo 9**) e alle informazioni relative ai reati o alle condanne penali (**articolo 10**).

Riportiamo le definizioni contenute nella normativa.

Dati genetici: sono i dati relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica, che forniscono informazioni univoche sulla sua fisiologia o sulla sua salute, e sono desumibili in particolare dall'analisi di un suo campione biologico.
Dati biometrici: sono i dati ottenuti da un trattamento tecnico specifico che forniscono informazioni relative alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica, consentendone o confermandone l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.
Dati relativi alla salute: sono i dati attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.
Dati relativi a condanne penali o reati: sono i dati relativi alle condanne penali, ai reati o a connesse misure di sicurezza.

Il trattamento delle categorie particolari di dati personali di cui al citato **articolo 9** è sempre vietato a meno che:

- **l'individuo abbia prestato il proprio consenso esplicito al trattamento di tali dati per finalità specifiche;**
- il trattamento sia necessario per assolvere gli obblighi ed esercitare i diritti specifici del Titolare del t rattamento o dell'individuo in materia di diritto del lavoro e della sicurezza sociale e protezione sociale;

- **il trattamento sia necessario per tutelare un interesse vitale di un individuo o di un'altra persona fisica qualora l'individuo si i trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;**
- Il trattamento sia effettuato da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con dette entità, avvenga in relazione a fini che sono loro propri e che i dati personali non siano comunicati all'esterno senza il consenso dell'individuo;
- il trattamento riguardi dati personali resi manifestamente pubblici dall'individuo;
- il trattamento sia necessario per accertare, esercitare o difendere un diritto in sede giudiziaria;
- il trattamento sia necessario per motivi di interesse pubblico;
- **il trattamento sia necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali** sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della Sanità, fatti salvi i casi in cui i dati sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale o da altra persona anch'essa soggetta all'obbligo di segretezza;
- **il trattamento sia necessario per motivi di interesse pubblico nel settore della Sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici;**
- il trattamento sia necessario a fini di archiviazione nel pubblico interesse, di **ricerca scientifica** o storica o a fini statistici, sia proporzionato alla finalità perseguita, rispetti l'essenza del diritto alla protezione dei dati e preveda misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'individuo.

Il trattamento di dati personali relativi a condanne penali e reati o a connesse misure di sicurezza di cui al citato **articolo 10** è sempre vietato a meno che esso avvenga sotto il controllo dell'autorità pubblica, oppure per autorizzazione del diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati.

3.2 —— Principi per il trattamento

Liceità, correttezza e trasparenza sono i principi a cui deve ispirarsi ogni operazione di trattamento di dati personali effettuata da Titolari e Responsabili del trattamento, che sono chiamati a rispondere della loro eventuale violazione.

I dati personali devono essere:

- raccolti per finalità determinate, esplicite e legittime (**limitazione delle finalità**);
- adeguati, pertinenti e limitati a quanto necessario per le finalità dichiarate e il loro trattamento deve essere sempre coerente con le medesime finalità (**minimizzazione dei dati**);
- esatti e, quando opportuno, aggiornati, anche per mezzo dell'adozione di misure idonee a cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati (**esattezza**);

- conservati in una forma che consenta l'identificazione degli individui per un periodo di tempo non eccedente il conseguimento delle finalità per le quali sono trattati. Possono essere conservati per periodi più lunghi se sono trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatta salva l'attuazione di misure tecniche e organizzative adeguate per tutelare i diritti e le libertà degli individui (**limitazione della conservazione**);
- trattati in maniera da garantire, con misure tecniche e organizzative apposite, la loro sicurezza e un adeguato livello di protezione nei confronti di trattamenti non autorizzati o illeciti, di eventuali perdite o di distruzione di informazioni e/o possibili danni accidentali (**integrità e riservatezza**).

Il rispetto dei suddetti principi impone al Titolare del trattamento, tra l'altro, l'adozione di comportamenti corretti e rispettosi delle norme e l'utilizzo di modalità di comunicazione chiare per tutta la durata delle operazioni di trattamento, fin dal momento della raccolta dei dati.

Le informazioni e le comunicazioni, fornite con un linguaggio semplice e chiaro, devono essere messe a disposizione di **tutte le entità coinvolte nei e dai** processi di trattamento, incluse quelle che svolgono operazioni di trattamento di dati personali per conto del Titolare del trattamento (quali ad esempio dipendenti, collaboratori o terze parti). La diffusione della cultura della protezione dei dati personale aumenta il livello di consapevolezza dell'organizzazione che opera e permette a tutti gli attori coinvolti nel processo di agire in modo informato, migliorando i comportamenti e, quindi, riducendo i rischi.

Il **comma 2 dell'articolo 5** stabilisce che "**Il Titolare del trattamento è competente**" per il rispetto dei principi applicabili al trattamento dei dati personali e, soprattutto, che è in grado di comprovarlo.

Non è un caso che il riferimento al principio di responsabilizzazione (**accountabilty**) sia stato definito esplicitamente nell'articolo 5, laddove sono definiti i principi applicabili al trattamento dei dati personali.

È un richiamo fondamentale, perché l'assolvimento degli obblighi in capo a coloro che effettuano il trattamento di dati personali è in qualche modo basato sul principio di responsabilizzazione e non sarà possibile sottrarvisi. Tutti coloro che effettuano trattamenti di dati personali dovranno anzi essere pronti a dimostrare, fornendo l'evidenza delle scelte effettuate e delle azioni intraprese, di aver svolto i propri compiti in modo lecito, corretto e trasparente nel rispetto di tutti i principi richiamati nell'**articolo 5** della normativa.

3.3 ——— Il registro dei trattamenti

3.3.1 ——— L'articolo 30 del Regolamento

Riferimento Normativo:

1. *Ogni Titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni:*

   a) il nome e i dati di contatto del Titolare del trattamento e, ove applicabile, del conTitolare del trattamento, del rappresentante del Titolare del trattamento e del responsabile della protezione dei dati;

   b) le finalità del trattamento;

   c) una descrizione delle categorie di interessati e delle categorie di dati personali;

   d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;

e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;

f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;

g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

2. *Ogni responsabile del trattamento e, ove applicabile, il suo rappresentante tengono un registro di tutte le categorie di attività relative al trattamento svolte per conto di un Titolare del trattamento, contenente:*

   a) il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni Titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del Titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;

   b) le categorie dei trattamenti effettuati per conto di ogni Titolare del trattamento;

   c) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;

   d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

3. *I registri di cui ai paragrafi 1 e 2 sono tenuti in forma scritta, anche in formato elettronico.*
4. *Su richiesta, il Titolare del trattamento o il responsabile del trattamento e, ove applicabile, il rappresentante del Titolare del trattamento o del responsabile del trattamento mettono il registro a disposizione dell'autorità di controllo.*
5. *Gli obblighi di cui ai paragrafi 1 e 2 non si applicano alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10.*

3.3.2 ——— Ratio della norma

La tenuta di un registro delle attività di trattamento rappresenta non solo uno dei primi adempimenti obbligatori previsti dal Regolamento UE 2016/679, ma soprattutto uno strumento operativo e funzionale alla gestione organica e sistematica dei dati trattati. Obbliga infatti ad avere un censimento sempre aggiornato dei dati trattati, un elenco ordinato degli archivi (o delle base dati) che contengono i dati, una classificazione delle categorie degli interessati coinvolti nonché una completa mappatura di tutti gli elementi rilevanti di un trattamento di dati personali per assicurare non solo un impianto di Data Protection in linea con i diversi requisiti normativi, ma anche un controllo reale, puntuale ed effettivo delle attività svolte. Oltre alla sua natura di strumento operativo di lavoro ex ante, *la costituzione e l'aggiornamento del registro*

delle attività rappresenta anche un ***importante documento probatorio*** *ex post da esibire in caso di verifica da parte dell'Autorità di Controllo* al fine di dimostrare - nell'ottica del principio di accountability - la compliance al GDPR. Non si dimentichi che la mancata tenuta del registro delle attività di trattamento può essere soggetta alla sanzione amministrativa pecuniaria fino a 10 milioni di euro.

Tanto premesso, la costruzione sistematica del registro, che "*è tenuto in forma scritta, anche in formato elettronico*", rappresenta un task che richiede un impegno significativo, soprattutto in alcuni settori come quello sanitario nel quale vengono trattati e prodotti dati in grande quantità e con un livello di alta "sensibilità", nonchè in considerazione del fatto che tale strumento potrebbe essere definito con livelli di automatizzazione e sofisticatezza differenti nei diversi contesti di riferimento. In quelli particolarmente complessi potrebbe essere anche consigliabile l'adozione di strumenti integrati o formulari semi-automatizzati, che consentano di alimentare e aggiornare direttamente il formato elettronico di tale registro, fatta salva la validazione del compilatore che lo rende valido ed efficace.

Poter far riferimento a linee metodologiche a cui attingere rappresenta di certo un valore, ma è altrettanto necessario che ogni entità, in virtù delle proprie specificità, sia autonomo operativamente nelle scelte del modello di rappresentazione delle attività di trattamento che rispecchi più fedelmente e in modo altamente funzionale il proprio sistema di gestione in conformità ai vincoli di contenuto e forma dettati dalla normativa.

Nel presente documento si tenta di fornire, pertanto, degli elementi guida generali per una più agevole individuazione delle caratteristiche fondamentali del processo di redazione, gestione e aggiornamento del registro delle attività di trattamento facendo riferimento ai possibili approcci supportati da alcuni esempi concreti inerenti al settore sanitario.

3.3.3 ——— Soggetti tenuti a dotarsi di un registro

Secondo quando previsto dal GDPR, l'obbligo della tenuta di un registro delle attività di trattamento non incomberebbe su tutte le imprese o organizzazioni Titolari o Responsabili dei dati, ma solo sulle imprese o organizzazioni con almeno di 250 dipendenti. Tuttavia saranno, altresì, **obbligate** a dotarsi di un registro quelle imprese o organizzazioni che, a prescindere dal numero di dipendenti:

- effettuino attività di trattamento che possano presentare un rischio per i diritti e le libertà dell'interessato
- effettuino attività di trattamento non occasionale o di ***categorie particolari di dati*** o i dati personali relativi a condanne penali e a reati.

L'Autorità garante italiana per la protezione dei dati personali si è altresi espressa in modo netto su quanti dovranno adottare il registro del trattamento all'interno delle Linee Guida[12] pubblicate la scorsa primavera, raccomandando:

"La tenuta del registro dei trattamenti non costituisce un adempimento formale bensì ***parte integrante di un sistema di corretta gestione dei dati personali****. Per tale motivo, si invitano tutti i titolari di trattamento e i responsabili, a prescindere dalle dimensioni dell'organizzazione, a compiere i passi necessari per dotarsi*

12. www.garanteprivacy.it/approccio-basato-sul-rischio-e-misure-di-accountability-responsabilizzazione-di-titolari-e-responsabili

di tale registro e, in ogni caso, a compiere un'accurata ricognizione dei trattamenti svolti e delle rispettive caratteristiche - ove già non condotta. I contenuti del registro sono fissati, come detto, nell'art. 30; tuttavia, niente vieta a un Titolare o responsabile di inserire ulteriori informazioni se lo si riterrà opportuno proprio nell'ottica della complessiva valutazione di impatto dei trattamenti svolti. Nello specifico, si richiama l'attenzione sulla sostanziale ***coincidenza fra i contenuti della notifica dei trattamenti di cui all'art. 38 del Codice e quelli che devono costituire il registro dei trattamenti ex art. 30 regolamento****; l'Autorità sta valutando di mettere a disposizione un modello di registro dei trattamenti sul proprio sito, che i singoli titolari potranno integrare nei modi opportuni. "*

È indubbio pertanto che tutte le strutture sanitarie in qualità di Titolari del Trattamento dati nonché tutte le imprese che rivestono il ruolo di Responsabili del trattamento dati in quanto trattano dati particolari per conto di strutture sanitarie, dovranno dotarsi obbligatoriamente di un registro dei trattamenti.

3.3.4 ——— Contenuti del registro

I comma 1 e 2 dell'articolo 30 del GDPR dettagliano - come di seguito riportato - i contenuti "minimi" del registro del Titolare del trattamento e del registro del Responsabile del trattamento.

REGISTRO DEL Titolare

a) *il nome e i dati di contatto del Titolare del trattamento e, ove applicabile, del conTitolare del rappresentante del Titolare del trattamento e del responsabile della protezione dei dati;*
b) ***le finalità del trattamento;***
c) ***una descrizione delle categorie di interessati e delle categorie di dati personali;***
d) ***le categorie di destinatari*** *a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;*
d) *le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;*
e) *ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;*
f) ***ove possibile, i termini ultimi previsti per la cancellazione*** *delle diverse categorie di dati;*
g) *ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.*

REGISTRO DEL RESPONSABILE

a) *il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni Titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del Titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;*

b) ***le categorie dei trattamenti*** *effettuati per conto di ogni Titolare del trattamento;*

c) *ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;*

d) *ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.*

Come risulta evidente dalle parti in grassetto dell'elenco soprariportato, i due registri non hanno identico contenuto: solo il Titolare del Trattamento deve dettagliare anche le finalità, le categorie di interessati, di dati personali trattati, di soggetti cui i dati possono essere comunicati e i tempi di data retention. Sono tutti gli elementi "distintivi" di un trattamento dati e che, non possono essere decisi da un Responsabile del trattamento, pena l'assunzione di fatto dello *status* di Titolare, con tutte le responsabilità tipiche che ne derivano (art. 28 c. 10).

Le informazioni che invece possono essere speculari in entrambi i registri, laddove il trattamento viene svolto dal Responsabile per conto del Titolare sono, oltre a quelli generali di descrizione del trattamento e dei soggetti coinvolti, le misure di sicurezza tecniche ed organizzative messe in atto per garantire ed essere in grado di dimostrare che il trattamento è effettuato conformemente al GDPR e gli eventuali trasferimenti verso paesi terzi con il dettaglio delle garanzie adeguate in conformità a quanto disciplinato negli artt. 46 e seguenti del GDPR.

È consigliabile che il registro delle attività di trattamento contenga tutta una serie di informazioni ulteriori rispetto a quelle minime previste nel comma 1 e 2 dell'art. 30, quali ad es: la base giuridica su cui si fonda il trattamento, le modalità di raccolta del consenso, l'elenco dei database e degli applicativi utilizzati, la filiera di tutti soggetti coinvolti nel trattamento (responsabili, sub-responsabili), ecc. in quanto sono fondamentali per contribuire alla formazione di un sistema documentale privacy quanto più possibile organico e completo. Si pensi ad esempio all'atto di nomina del Responsabile del trattamento, alle istruzioni da fornire alle persone autorizzate al trattamento o ancora alle informative da rendere agli interessati, che devono obbligatoriamente contenere alcune delle informazioni tratte dal Registro delle attività di trattamento. Vi è anche da ricordare come sia necessario approcciare all'elencazione delle attività tenendo conto dei contenuti dell'attuale registro delle notificazioni.

3.3.5 ——— Strutturare i registri: un possibile approccio metodologico

La mappatura delle attività di trattamento dei dati correlate ai diversi processi può essere condotta mediante una primaria attività di ricognizione di tutte le informazioni correlate ai trattamenti dei dati di cui già l'organizzazione tiene traccia (per finalità privacy o distinte) all'interno dell'organizzazione. A tal proposito le informazioni necessarie possono essere reperite da:

- mappatura dei processi della impresa/organizzazione in cui sono riportate le attività di trattamento (ad es. procedure interne)

- ricognizione delle schede dei trattamenti precompilate
- recupero delle informazioni contenuto nell'ultimo DPS disponibile, opportunamente riviste e/o validate dal referente dell'area dove viene svolto lo specifico trattamento e dei sui collaboratori (ad es. un reparto ospedaliero, ufficio risorse umane ecc.)
- assessment puntuale dei trattamenti e dei data flows interni ed esterni

La mappatura delle attività di trattamento dei dati correlate ai diversi processi di una organizzazione strutturata in ambito sanitario può essere altresì definita mediante **un confronto (interviste)** con i referenti ed i collaboratori delle diverse unità organizzative che presidiano tali processi (es. direzione sanitaria, direzione scientifica, direzione amministrativa, direzione risorse umane) al fine di raccogliere tutte le informazioni utili quali i servizi esternalizzati, i sistemi di controllo, gli applicativi in uso, le misure di sicurezza poste in essere, ecc.

In una prospettiva di Data Governance, si possono classificare le informazioni raccolte come "**cataloghi di metadati**", come ad esempio il catalogo delle "categorie di interessati" (es. Pazienti, Minori, Fornitori, Dipendenti, Collaboratori Esterni, etc.) o il catalogo delle "categorie di destinatari" a cui i dati personali sono stati o saranno comunicati (Centri di ricerca UE/ Extra UE, Università UE/ Extra UE, Autorità di Vigilanza, ecc.) e così via. In questo senso, dunque, il Registro dei Trattamenti può essere realizzato alla stregua di un **Repository di Metadati** e implementato avvalendosi di strumenti già in uso (es. Data Dictionary/ Business Glossary, Meta-data Repository, etc.) e metodologie già messe a disposizione dai programmi di Data Governance già avviati dalla organizzazione.

Inoltre, la redazione del contenuto del Registro potrà essere agevolata dalla ricognizione ed utilizzo di altre informazioni attinenti:

- l'elenco dei **processi di business e IT**;
- l'elenco delle **applicazioni** che supportano tali processi;
- il **catalogo dei rischi operativi e IT** connessi a tipologie di dati e di processi.

Con riferimento più in generale alle attività di ricognizione delle informazioni connesse ai trattamenti potrà farsi riferimento a checklist privacy standard e *best practice* eventualmente esistenti nel settore di riferimento anche alla luce delle indicazioni dell'Autorità Garante nell'ambito Sanità.

3.3.6 —— Aggiornamento e messa a disposizione dei registri

Il registro dei trattamenti dovrebbe essere aggiornato con regolarità posto che deve costituire una rappresentazione realistica dei trattamenti posti in essere e di tutti gli aspetti correlati oggetto di attenzione da parte del Regolamento (finalità, eventuali trasferimenti verso paesi terzi ecc.).
In particolar modo, sarà necessario provvedere ad un aggiornamento del registro in presenza di ogni cambiamento organizzativo, operativo e tecnologico rilevante e tale da impattare sulla gestione dei dati personali.

A tal fine, è raccomandabile istituire dei **flussi informativi** periodici e all'occorrenza verso il soggetto o l'unità organizzativa preposta all'aggiornamento del Registro.

Tali flussi potranno essere dunque attivati da:

Direzione Sanitaria

Direzione Sistemi informativi

Direzione Scientifica

Direzione Comunicazione e Marketing

Direzione Customer Service

Direzione Amministrazione, Finanza e Controllo

Direzione Risorse Umane e Organizzazione

Direzione Acquisti

3.4 —— Tenuta del registro

La tenuta del registro è in capo al Titolare ed al Responsabile che saranno generalmente coloro che appongono le firme e/o eseguono gli atti necessari a dare forma probatoria al registro. In ogni caso, in conformità a quanto previsto dal WP243, paragrafo 4.5 "*niente vieta al Titolare o al responsabile del trattamento di affidare al RPD il compito di tenere il registro delle attività di trattamento sotto la responsabilità del Titolare o del responsabile stesso.*". Peraltro al paragrafo 2.5 dello stesso documento, riguardante le conoscenze e le competenze del DPO, si chiarisce come per lo stesso, riguardo alle capacità di assolvere i propri compiti *"si deve intendere sia quanto è legato alle qualità personali e alle conoscenze del RPD, sia quanto dipende dalla posizione del RPD all'interno dell'azienda o dell'organismo. Le qualità personali dovrebbero comprendere, per esempio, l'integrità ed elevati standard deontologici; il RPD dovrebbe perseguire in via primaria l'osservanza delle disposizioni del RGPD. Il RPD svolge un ruolo chiave nel promuovere la cultura della protezione dei dati all'interno dell'azienda o dell'organismo, e contribuisce a dare attuazione a elementi essenziali del regolamento quali i principi fondamentali del trattamento[26], i diritti degli interessati[27], la protezione dei dati sin dalla fase di progettazione e per impostazione predefinita[28], i registri delle attività di trattamento[29], la sicurezza dei trattamenti[30] e la notifica e comunicazione delle violazioni di dati personali.[31]*

3.5 —— Inventario degli asset tecnologici

Una buona gestione dell'inventario è un presupposto per l'efficacia e l'efficienza di molti processi di gestione. Nel caso dell'adeguamento al GDPR, costituisce il collegamento fra il Registro dei trattamenti, che è il punto di partenza per individuare gli ambiti applicativi ed i flussi interessati, e il sistema informativo in quanto insieme di asset tecnologici. Un buon inventario è però in generale uno strumento di gestione importante a supporto di molti processi. Ad esempio, la gestione degli incidenti, il change management, la gestione delle vulnerabilità e delle relative attività di remediation, sono tutti processi che traggono un gran-

26. Capo II
27. Capo III
28. Art. 25.
29. Art. 30.
30. Art. 32.
31. Artt. 33 e 34

de vantaggio dall'esistenza di un inventario quanto più completo ed aggiornato. Si tratta anzi di strumenti che spesso sono integrati ad esempio in strumenti di IT Service Management, dei quali costituiscono un componente essenziale.

L'introduzione di un inventario, dove non sia già disponibile, è però notoriamente complessa ed onerosa. Il primo presupposto perché non sia un'iniziativa sterile e destinata al fallimento, è che ci sia un effettivo controllo sui cambiamenti al sistema informativo, prima ancora che una mappatura dello stato esistente. Senza entrare ulteriormente nel merito di questo tipo di iniziative, vediamo il ruolo dell'inventario nella gestione della conformità al GDPR.

Il primo e più importante aspetto riguarda la capacità di associare i trattamenti agli asset che li supportano: sistemi e applicativi principalmente, ma anche componenti infrastrutturali. Nella predisposizione del registro dei trattamenti infatti, in prima battuta i diversi responsabili daranno una propria visione di quelli che sono gli applicativi (che potremmo indicare più genericamente come "ambiti applicativi") a supporto del trattamento. Questa prospettiva è necessariamente di livello più alto rispetto a quella della Direzione sistemi informativi, che a fronte ad esempio di un applicativo indicato dal Responsabile, dovrà sapere che in realtà c'è potenzialmente un insieme di applicazioni ed asset tecnologici che lo compongono. Ad esempio, il responsabile tipicamente vedrà un'interfaccia, magari web in un portale, ed indicherà il componente del portale come "applicativo" interessato. Questo applicativo dovrà essere mappato sull'insieme di componenti che lo supportano. Analogamente, quando il responsabile indica un insieme di applicativi, dovranno essere individuati i diversi asset interessati dai diversi flussi fra gli applicativi stessi. È evidente come questa mappatura richieda di disporre di un inventario aggiornato degli asset e dei flussi corrispondenti.

Da un punto di vista operativo, quello stesso inventario sarà a supporto ad esempio degli interventi di adeguamento: laddove ad esempio un provvedimento del Garante, un'evoluzione del rischio o una modifica ad un trattamento ci richiedano di intervenire sui sistemi a supporto di uno o più trattamenti, l'inventario è quello che permetterà di assicurare la completezza del perimetro su cui le modifiche saranno effettuate.

Infine, in caso di data breach, nella direzione opposta, a fronte della compromissione di uno o più sistemi, sarà possibile individuare con la tempestività richiesta i trattamenti potenzialmente impattati. Questo aspetto è anche presupposto necessario per una gestione della sicurezza in generale, e quindi della conformità all'art. 32 del GDPR: è necessario ad esempio per individuare i sistemi interessati da una vulnerabilità relativa ad una specifica versione di sistema operativo, nonché per valutare correttamente le segnalazioni di un sistema di intrusion detection o di monitoraggio eventi in generale.

In questa prospettiva, è particolarmente importante un inventario degli applicativi, dei database e dei middleware, nonché dei sistemi a supporto, che comprenda le versioni dei software e lo stato di aggiornamento (anche di strumenti di sicurezza come gli antivirus). Queste informazioni si devono integrare con una mappa dei flussi applicativi. Non entreremo nel merito della struttura di un tale inventario, la cui realizzazione, anche tenendo conto dell'onerosità di realizzazione e aggiornamento, dovrà necessariamente essere a supporto della gestione del sistema informativo in generale, e non una misura di semplice conformità. Il settore sanitario tratta e produce dati in grande quantità e con un livello di alta "sensibilità". La corretta e sicura gestione dei dati dei pazienti, in particolare quelli idonei a rilevare lo stato di salute, deve essere finalizzata ad assicurarne al contempo la confidenzialità, l'inviolabilità e la protezione al fine di prevenire danni materiali e morali all'individuo come ad es. ipotesi di discriminazioni.

4 ——— Analisi dei rischi e degli impatti

4.1 ——— Analisi dei rischi

4.1.1 ——— Analisi preliminare del rischio

Il GDPR prevede in capo al Titolare del trattamento l'onere di procedere ad una valutazione oggettiva del rischio, avendo riguardo della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento. Da tale valutazione sarà possibile stabilire che tipo di rischio comporti qualsivoglia trattamento di dati. È utile però precisare che vi sono due tipologie di analisi previste all'inerno del GDPR, distinte e complementari. Una è il Data Protection Impact Assessment (DPIA), che è un'analisi degli impatti (non del rischio) volta ad individuare i trattamenti che presentino un rischio elevato per i diritti e le libertà delle persone fisiche, riconducibile all'art. 35 del GDPR. La DPIA può portare all'esigenza di adottare delle misure di sicurezza volte ad attenuare adeguatamente il rischio.
La seconda analisi, riconducibile principalmente all'art. 32 del GDPR, è un'analisi del rischio, che ha lo scopo di valutare in generale l'adeguatezza delle misure di sicurezza volte ad attenuare il rischio per i dati personali. Questa seconda analisi, a differenza della prima, è dovuta in generale laddove avvenga un trattamento di dati personali (lo sarà a maggior ragione dove la DPIA avrà individuato degli impatti potenzialmente elevati). Posto che la crescente digitalizzazione dei processi, sia nel settore privato che in quello pubblico, genera costantemente nuovi scenari di rischio (informatico e non solo), sia all'interno che all'esterno delle organizzazioni, il GDPR, focalizzandosi sulla protezione dei dati personali, evoca la necessità di un cambiamento significativo nell'approccio di gestione degli stessi. Ciò, in particolare, perché le nuove tecnologie consentono di erogare servizi sempre più personalizzati per i cittadini, ma nel contempo aumentano la complessità e la pervasività dei trattamenti di dati personali svolti nell'ambito dell'erogazione di tali servizi.
Nella presente sezione saranno indicati dei possibili approcci metodologici per valutare i rischi inerenti ai trattamenti e valutare, dunque, l'adeguatezza delle misure per la limitazione di tali rischi.

Riferimenti normativi

Considerando (76) GDPR

La probabilità e la gravità del rischio per i diritti e le libertà dell'interessato dovrebbero essere determinate con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento. Il rischio dovrebbe essere considerato in base a una valutazione oggettiva mediante cui si stabilisce se i trattamenti di dati comportano un rischio o un rischio elevato.

Considerando (83) GDPR

Per mantenere la sicurezza e prevenire trattamenti in violazione al presente regolamento, il Titolare del trat-

tamento o il responsabile del trattamento dovrebbe valutare i rischi inerenti al trattamento e attuare misure per limitare tali rischi, quali la cifratura. Tali misure dovrebbero assicurare un adeguato livello di sicurezza, inclusa la riservatezza, tenuto conto dello stato dell'arte e dei costi di attuazione rispetto ai rischi che presentano i trattamenti e alla natura dei dati personali da proteggere. Nella valutazione del rischio per la sicurezza dei dati è opportuno tenere in considerazione i rischi presentati dal trattamento dei dati personali, come la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati a dati personali trasmessi, conservati o comunque elaborati, che potrebbero cagionare in particolare un danno fisico, materiale o immateriale.

Art. 32 GDPR

1. *Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il Titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:*
   a) la pseudonimizzazione e la cifratura dei dati personali;
   b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
   c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
   d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
2. *Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati. […]*

4.1.2 ——— Una necessaria considerazione sui principi generali di data protection in relazione all'analisi del rischio

Il trattamento dei dati personali deve essere conforme ai principi generali previsti dal Regolamento nonché dalle prescrizioni del Garante privacy nei settori di riferimento (come ad es. quello sanitario).
È bene notare come questi principi devono trovare piena soddisfazione a prescindere dal livello di rischio stimato tramite analisi del rischio e valutazione degli impatti del trattamento. In sostanza, l'insieme di tali principi costituisce lo sfondo di ogni valutazione di impatto che il Titolare del trattamento effettuerà. In ogni caso, naturalmente, l'attuazione di questi principi generali, sarà in concreto verificabile in corrispondenza del livello di rischio riscontrato per il trattamento oggetto di valutazione.

Liceità e correttezza	••La liceità corrisponde all'ottemperamento del dovere di correttezza che comprende non solo lo scopo d'utilizzo ma anche le modalità di raccolta
Finalità	••I dati raccolti per una finalità specifica non possono essere utilizzati per altri scopi
Minimizzazione	••Raccogliere e trattare solo le informazioni essenziali per il raggiungimento dello scopo
Pertinenza e completezza	••I dati che si raccolgono devono essere pertinenti allo scopo dichiarato e non devono risultare incompleti o parziali
Esattezza e aggiornamento	••I dati devono corrispondere a informazioni esatte e aggiornate
Durata	••Il tempo di conservazione del dato è strettamente connesso al perseguimento della finalità

Figura: I principi a sfondo della DPIA - Fonte:Deloitte

4.1.3 ——— Quando è necessario svolgere l'analisi dei rischi

Come indicato poco sopra, l'analisi dei rischi si configura nel GDPR come una attività funzionale al mantenimento della sicurezza e alla prevenzione di trattamenti in violazione delle prescrizioni ivi dettate.

Ciò posto, tale attività di analisi dei rischi va condotta sia per i nuovi trattamenti sia per tutti i trattamenti posti in essere dal Titolare avendo cura di provvedere ad una costante puntuale mappatura degli stessi utile a preservare un adeguato livello di sicurezza e prevenire in modo tempestivo eventuali non conformità al GDPR.

Naturalmente sarà anche utile procedere ad analizzare l'eventuale insorgere o aggravamento di rischi al prefigurarsi di un sopraggiunto cambiamento organizzativo, tecnologico o di processo che possa incidere significativamente sul livello di conformità alle previsioni del GDPR da parte di trattamenti già oggetto di mappatura ed analisi precedentemente al cambiamento intervenuto (anche al fine di aggiornare il Registro delle attività di trattamento).

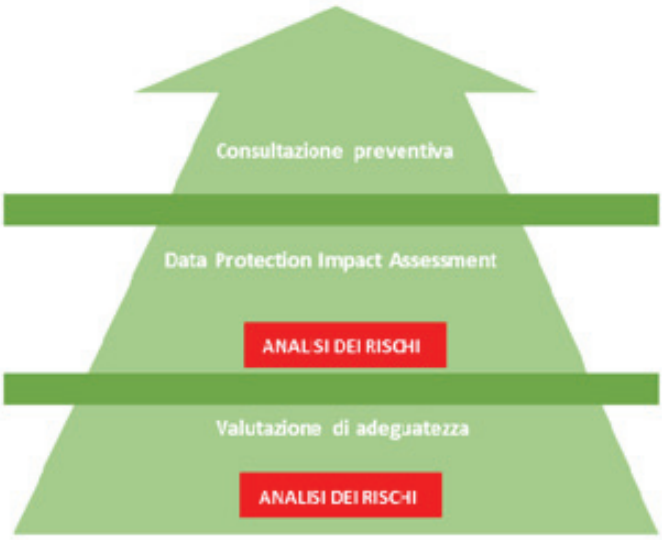


Figura: collocazione prodromica della fase di analisi del rischio nella piramide di attività di valutazioni poste dal Regolamento in capo al Titolare - Fonte: Deloitte

4.1.4 ——— Rischio inerente e rischio residuo

La carente sicurezza dei dati e dei sistemi può rappresentare una causa esiziale di malasanità mentre, per converso, la protezione dei dati e dei sistemi costituisce un fattore determinante di efficienza sanitaria. Il processo di digitalizzazione della Sanità (c.d. E-Health) non può non andare di pari passo con una attività sempre più puntuale di valutazione dei rischi connessi all'uso di nuove tecnologie in questo ambito, rispetto al quale l'assenza di valutazioni preventive della pericolosità di un trattamento o di un piano organico di sicurezza mette a rischio non solo banche dati essenziali ma, insieme, viola quanto di più intimo vi è nella persona esponendola a gravi conseguenze (a titolo di esempio, discriminazioni, stato di ansia e paura, danni biologici ecc.).

I rischi che il trattamento di dati personali può astrattamente sollevare riguardo ai diritti e alle libertà dei soggetti, ai quali si riferiscono le informazioni raccolte e utilizzate, devono essere considerati nell'ambito delle attività di analisi nell'ottica di "probabili conseguenze". Queste ultime potranno essere identificate come:

- danni materiali (ad es. un danno fisico)
- danni immateriali (ad es. discriminazione).

In primo luogo, dovrà essere rilevato il rischio inerente ad un trattamento (cioè la combinazione tra la gravità della conseguenza, in astratto configurabile, e la probabilità del suo accadimento in assenza di misure atte a ridurlo; nella pratica, in una valutazione del rischio IT si tendono a considerare comprese invece le misure di sicurezza "non IT", tipicamente a livello di processo), e si procederà poi ad un confronto con le caratteristiche e modalità fattuali del tipo di trattamento oggetto di analisi.
In secondo luogo, andranno individuate le misure appropriate per minimizzare il livello di rischio per il trattamento rilevato, nell'ottica di conformità rispondente a principi di scalabilità e proporzionalità (come si vedrà meglio nel proseguo). L'adozione delle misure a garanzia dei diritti e delle libertà degli interessati permetterà di valutare come il rischio inizialmente configurabile in astratto come inerente al trattamento possa essere concretamente mitigato.
A questo punto, sarà possibile valutare l'eventuale livello di rischio residuo (ovverosia la porzione residuale di rischio ponderata appunto in considerazione delle misure individuate).

4.1.5 ——— Analisi preliminare del rischio e prospettiva garantista

Nell'ambito della Sanità elettronica, da un'attenta ricerca condotta sulle priorità fissate dall'Autorità Garante in questo ambito (si faccia riferimento alle Relazioni annuali del Garante privacy), emerge quella di assicurare la massima ***protezione dei dati sanitari dei pazienti favorendo al contempo lo sviluppo di nuove tecnologie*** *nella cura delle persone. Ciò comporta che tutte le strutture sanitarie Titolari di trattamenti di dati personali, dovranno porsi nella stessa prospettiva garantista incentrata sui diritti dell'interessato, operando continui bilanciamenti tra i benefici connessi all'uso delle tecnologie e i rischi potenzialmente lesivi dei diritti e delle libertà dei pazienti.*

A tal proposito si suggerisce in primo luogo di far riferimento alle regole e prescrizioni dettate negli anni dal Garante privacy nell'ambito di specifici settori o tematica poste sotto la lente di ingrandimento dell'Autorità

garante in quanto con potenziale alto livello di rischio. In particolare si fa riferimento ai seguenti ambiti:

- *fascicolo sanitario elettronico*
- *dossier sanitario elettronico*
- *refertazione on line*
- *monitoraggio a distanza dei pazienti portatori di defibrillatori cardiaci*
- *prenotazione di visite specialistiche (es. presso i Cup e presso le farmacie)*
- *interconnessione delle banche dati.*
- *IoT*

L'obiettivo primario delle prescrizioni del Garante privacy, in perfetta ***assonanza con le previsioni del Regolamento****, è quello di garantire che le strutture sanitarie che raccolgono, usano, conservano i dati lo facciano avendo preventivamente sotto controllo l'entità del rischio per ogni attività di trattamento -operato in un contesto di E-Health- sia preventivamente valutato per provvedere all'attività in sicurezza sotto il profilo della protezione dei dati.*

L'analisi dei rischi di un trattamento sulla protezione dei dati deve tener conto del processo in cui viene operato il trattamento dei dati, potendosi distinguere tra processi principali e di supporto all'organizzazione sanitaria. Esempi di macroaree di processo principale sono: la formazione del personale e l'audit interno (strategici), i servizi diagnostici e l'accettazione (operativi), mentre esempio di un'area di processo di supporto può essere individuate nella gestione dei fornitori.

È importante, quindi, da un punto di vista metodologico, avviare l'analisi dei rischi partendo da una puntuale mappatura dei processi.

Figura: esempio di classificazione dei macroaree di processo nelle organizzazioni afferenti al sistema sanitario

Susseguentemente, al fine di **determinare il profilo di rischio di un tipo di trattamento** (con successiva valutazione della necessità o meno di avviare una valutazione d'impatto sulla privacy di quel trattamento) è utile tenere presente:

- le casistiche previste dal GDPR;
- le casistiche previste dalle Linee Guida del Gruppo ex art. 29 -wp 248-(denominato "WP29");
- le risultanze dell'analisi di adeguatezza dei presidi operate nell'ambito di ulteriori attività di analisi dei rischi (ad es. analisi condotte nell'ambito del Sistema di gestione della qualità, analisi dei rischi cyber relativi all'uso di ICT ecc.);
- ulteriori indicazioni che potranno giungere dall'European data privacy board (EDPB).

In proposito si segnala che il GDPR prevede la possibilità di effettuare la DPIA in base al livello di rischio. In tale contesto si evdienzia **che in Sanità, la tipologia di dati trattati e la complessità dei processi organizzativi supportati da ICT che, nella stragrade maggioranza dei casi, richiedono continuità operativa h24, è altamente probabile che la maggior parte dei trattamenti siano a rischio elevato. Di conseguenza si suggerisce di effettuare "by default" un'analisi di rischi e impatti per ogni macroprocesso operativo nel quale vengono trattati dati personali e sensibili. Come già citato, questa attività di valutazione dei rischi e degli impatti sarà utilizzabile anche per il Piano di continuità operativa che è un procedimento obbligatorio per tutte le Pubbliche Amministrazioni.**

Infine, nella valutazione dei potenziali rischi che possono inerire specifici ambiti di attività delle strutture, si suggerisce di far riferimento agli interventi dell'Autorità Garante per la protezione dei dati personali e del Legislatore che normano alcune delle applicazioni dell'e-Health, agevolandone lo sviluppo e al contempo prescrivendo gli idonei livelli di garanzia. Si segnala, a titolo esemplificativo e non esaustivo, l'attenzione posta di recente sul tema del Dossier sanitario (si segnala il *Provvedimento del Garante privacy n. 331 del 4 giugno 2015) nonché sul tema della Telemedicina (si faccia riferimento al documento "Telemedicina - Linee di indirizzo nazionali" del 20 febbraio 2014 approvato dalla Conferenza Stato-Regioni).*

4.1.6 ——— Analisi dei rischi: considerazione tecniche

Secondo la norma ISO 31000 "Gestione del rischio", di riferimento in materia di rischio per tutta la famiglia di norme ISO, il rischio è l'**effetto** dell'**incertezza** sugli obiettivi. Questa definizione è in linea con il concetto più comune ed informale che descrive il rischio come funzione di una **probabilità** (l'incertezza) e di un **impatto** (l'effetto). Anche il GDPR si richiama agli stessi concetti quando, ad esempio nell'art. 32, richiama il "rischio di varia **probabilità** e **gravità** per i diritti e le libertà delle persone fisiche".

L'analisi dei rischi richiede quindi di valutare sia la componente probabilistica che quella di impatto. Si tratta in generale di stime, in quanto le valutazioni su possibili eventi del futuro comportano sempre un'aleatorietà molto difficile da quantificare.

L'analisi di impatto comprende due prospettive: quella della DPIA, richiesta esplicitamente dal GDPR, e quella dell'impatto sui processi aziendali data da possibili incidenti di sicurezza. Quest'ultima è richiesta per valutare l'adeguatezza delle misure di sicurezza adottate. Si tratta quindi di due prospettive diverse, entrambe da considerare per individuare i componenti del sistema informativo la cui compromissione avrebbe un impatto importante sui processi aziendali (e quindi di nuovo, indirettamente, anche sui dati personali) o sugli

interessati. Mentre le valutazioni di impatto sono a carico principalmente dei responsabili dei diversi processi, le valutazioni di probabilità, tolta una valutazione "generica" di rischiosità dell'ambito di attività dell'azienda, è maggiormente di competenza del Responsabile del Sistema informativo. Per semplificare l'esecuzione della DPIA e la valutazione di impatto di sicurezza sui processi aziendali, può essere utile fare riferimento a delle fasce di impatto. L'obiettivo di questa attività consiste nel formulare ipotesi condivise circa la gravità deli impatti e la pobabilità di accadimento per poi individuare il rischio ad es. con una heatmap come quella rappresentata nella figura seguente.

Heatmap

Probabilità					
Alta	Medio	Medio	Alto	Molto alto
Media	Basso	Medio	Alto	Molto alto
Bassa	Basso	Medio	Medio	Alto
Molto bassa	Basso	Basso	Medio	Medio
	Basso	Medio	Alto	Molto alto

Impatto

Nel valutare la componente probabilistica, dobbiamo rispondere alle seguenti domande:

Cosa voglio proteggere vale a dire identificazione dei Beni Aziendali o Asset Informativi (a)
Da cosa voglio proteggermi vale a dire identificazione delle Minacce (m)
Perché proteggermi vale a dire Identificazione delle Vulnerabilità (v)
Come proteggermi vale a dire misure Tecnico Organizzative e Applicative (controlli di sicurezza (c)

Il punto di partenza per un'analisi del Rischio è l'analisi del contesto e l'individuazione dei beni da proteggere, identificare le minacce, identificare le vulnerabilità e i controlli di sicurezza, rapportare le minacce alle vulnerabilità, definire l'impatto su ciasun bene in relazione al mancato rispetto dei requisiti quindi valutare il rischio per ciascun bene.

Il Rischio potrà essere calcolato attraverso una relazione del tipo:

Rischio(m,a,v) = probabilità(m,v)*impatto(m,a,v)

dove la vulnerabilità è inversamente proporzionale al controllo di sicurezza adottato (c).

Il passo successivo consiste quindi nell'identificazione delle minacce che possono determinare la gravità degli impatti.
La ISO/IEC 27000 dà questa definizione: *minaccia: causa potenziale di un incidente, che può comportare danni ad un sistema o all'organizzazione* dove incidente è relativo alla sicurezza delle informazioni e l'analisi del rischio richiede di identificare e valutare tutte le minacce relative alla sicurezza delle informazioni quindi non solo quelle informatiche o quelle più significative.

Abbiamo già visto *(Analisi preliminare del Rischio gruppo organizzativo)* che gli elementi di rischiosità che derivano dal Trattamento sui Dati e sulle quali dobbiamo concentrare l'attenzione sono quelli che portano alla:

- distruzione o non disponibilità
- perdita
- modifica
- divulgazione non autorizzata
- accesso accidentale o illegale

dei dati personali trasmessi, conservati o comunque trattati (art. 32 c.2 del GDPR)

Questi elementi di rischiosità possono essere sintetizzati attraverso i parametri della Terna RID:

- Riservatezza (R)
- Integrità (I)
- Disponibilità (D)

Per identificare le minacce le devo correlare ai parametri RID e poiché possono avere impatti su uno o più di questi parametri è utile utilizzare una struttura a matrice.
Per rendere sistematica l'analisi delle minacce, è opportuno inziare da una lista predefinita. Un elenco delle più comuni tecniche di minaccia informatica può essere integrato prendendo in considerazione almeno i seguenti item:

Minaccia	**R**	**I**	**D**
Malware	X	X	X
Diffusione Documenti	X		
Modifica scorretta Sistema IT	X	X	X
Furto di identità (credenziali)	X	X	X
Modifica non autorizzata di documenti informatici da non malintenzionati		X	
Modifica non autorizzata di documenti informatici da malintenzionati		X	
Attacchi di Denial of Service			X
Uso eccessivo e involontario delle risorse da parte degli utenti			X

Blackout elettrici		X	X
Guasto Impianto			X
Incendio		X	X
Ransomware	X	X	X
Lettura e copia non autorizzata di documenti digitali	X		
Invio di dati a persone non autorizzate	X		
Danneggiamento di apparecchiature fisiche	X	X	X
Danneggiamento dei programmi Informatici	X	X	X
Accesso non autorizzato ai sistemi IT	X	X	X
Furto di apparecchiature Informatiche o fisiche	X	X	X
Social Engineering	X	X	X
Lettura, furto copia o alterazione di documenti in formato fisico	X	X	X
Trattamento scorretto delle informazioni rispetto alla normativa	X		

Le minacce dovrebbero essere inizialmente individuate dai Referenti delle Informazioni o dai Responsabili di Processo ma la necessità di competenze specifiche e la loro natura probabilistica come cause potenziali di incidente rende necessario il convolgimento del Responsabile dei Sistemi Informativi, della Sicurezza, del Personale, dell'Ufficio Acquisti e dell'Uffcio Legale.

Senza identificare tutte le possibili vulnerabilità di un sistema informatico ci limitiamo ad elencare le tipologie più comuni che sono:

- vulnerabilità strutturali
- vulnerabilità legate all'architettura di rete
- vulnerabilità organizzative/procedurali
- vulnerabilità di sistemi/applicazioni
- vulnerabilità del software,overflow,format string
- errori di configurazione
- vulnerabilità dei protocolli
- debolezza di progettazione attacchi Spoofing, Hijacking, Sniffing
- errori implementazione dello stack di rete: attacchi Dos, DdoS

I controlli di sicurezza più utilizzati da mettere in atto per contrastarle sono quelli noti come:

- *Antivirus*
- *Antispyware*
- *Firewall*
- *Firma digitale, Crittografia*
- *Backup*
- *Intrusion Detection System (IDS)*
- *Network Intrusion Detection System (NIDS)*
- *Sistema di autenticazione/autorizzazione*

Dove il Rischio è elevato le misure di sicurezza applicate dovranno essere adeguate. Si ricorda a tal proposito come le linee guida del Garante in ambito dossier sanitario elettronico richiedano misure appropriate come:

- *Tracciabilità degli accessi e delle operazioni effettuate*
- *Sistemi di audit log*
- *Separazione e cifratura dei dati*
- *Data breach*
- *Data protection officer (visto dal punto di vista dell'entità oggettiva)*

Da un punto di vista operativo, l'analisi dei rischi è finalizzata a:

- *identificare i rischi maggiori, per i quali devono essere necessariamente adottate delle contromisure atte a mitigarli fino a ridurli ad un livello adeguato*
- *prioritizzare gli interventi, da effettuare anche in relazione alle risorse disponibili*
- *dare evidenza del rischio residuo, che i responsabili dei diversi processi dovranno esplicitamente accettare*

A fronte di risorse insufficienti o di vincoli di vario genere posti dall'azienda, deve infatti essere chiaro ed esplicito che la responsabilità del rischio residuo non rimane in generale in capo al Responsabile del sistema informativo, ma ai responsabili dei diversi processi aziendali nell'ambito dei quali sono individuati gli impatti.

4.1.7 ——— Ambito di applicazione della DPIA

La DPIA può riguardare una sola operazione di trattamento dei dati oppure una singola valutazione può affrontare una serie di operazioni di trattamento simili che presentano rischi simili elevati (come ad es. nel caso in cui una Struttura sanitaria voglia adottare un dispositivo tecnologico del tutto simile ad uno già in uso per raccogliere lo stesso tipo di dati per le medesime finalità).
Quando il trattamento coinvolga co-Titolari, essi devono definire i propri rispettivi obblighi con precisione e, in particolare, ogni DPIA eseguita deve indicare quale Titolare è responsabile per le varie misure individuate per mitigare i rischi.

4.1.8 ——— Come effettuare una DPIA: un possibile approccio metodologico

Abbiamo visto che il GDPR e le Linee guida del WP29 offrono esempi di casistica di trattamenti a rischio elevato e comunque in presenza di un tipo di trattamento che la struttura sanitaria vuole avviare che presenti

almeno due dei criteri di rischio riportati nella Tabella xxx sarà necessario effettuare una DPIA più complessa e dettagliata in rapporto a quel "tipo" di trattamento che si articolerà nelle sotto-fasi di seguito riportate:

Valutazione della probabilità totale di accadimento delle minacce

Analogamente a quanto avviene in caso di trattamento a rischio non elevato, lo scopo di questa fase è analizzare qualitativamente la probabilità di accadimento delle principali minacce che insistono sui dati personali. La probabilità di accadimento di tali minacce sarà connessa al livello di implementazione delle misure organizzative/operative e tecniche implementate a protezione dei dati personali.

Valutazione del livello di gravità per ogni binomio minaccia-danno

In questa fase, alla probabilità calcolata nella precedente fase 1, dovrà essere associata una valutazione della gravità per ciascun binomio minaccia - danno.

Essendo in presenza di un livello di rischio elevato ("Alto" nella scala di ponderazione) dovrà essere effettuata una valutazione più di dettaglio (appunto richiesta espressamente dall'art. 35 GDPR), valutando la gravità per una serie di danni ad un **livello di granularità maggiore** rispetto al caso dell'analisi preliminare di trattamenti a rischio non elevato.

In particolare, per i trattamenti a rischio elevato i danni considerati sono di due tipologie: danni materiali e danni immateriali, al riguardo si riporta di seguito *un esempio generale di matrice di alcuni potenziali impatti* per la protezione dei dati personali per trattamenti a rischio elevato:

MINACCE / DANNI	Uso improprio	Rischio Accesso non autorizzato	Rivelazione non autorizzata	Modifica non autorizzata	Perdita	Distruzione accidentale o illegale
MATERIALI						
Danni fisici	R_1=PxG	R_2=PxG	R_3=PxG	R_4=PxG	R_5=PxG	R_6=PxG
Danno emergente	R_7=PxG	R_8=PxG	R_9=PxG	R_{10}=PxG	R_{11}=PxG	R_{12}=PxG
Mancato guadagno	R_{13}=PxG	R_{14}=PxG	R_{15}=PxG	R_{16}=PxG	R_{17}=PxG	R_{18}=PxG
IMMATERIALI						
Discriminazione o stigmatizzazione	R_{19}=PxG	R_{20}=PxG	R_{21}=PxG	R_{22}=PxG	R_{23}=PxG	R_{24}=PxG
Danni a identità (furto, omonimia)	R_{25}=PxG	R_{26}=PxG	R_{27}=PxG	R_{28}=PxG	R_{29}=PxG	R_{30}=PxG
Reputazionali	R_{31}=PxG	R_{32}=PxG	R_{33}=PxG	R_{34}=PxG	R_{35}=PxG	R_{36}=PxG
Ansia/paura	R_{37}=PxG	R_{38}=PxG	R_{39}=PxG	R_{40}=PxG	R_{41}=PxG	R_{42}=PxG

Con riferimento alla gravità, essa dovrà essere valutata a livello qualitativo sulla base della scala di valutazione richiamata in sede di analisi preliminare di rischio.

Valutazione del rischio complessivo del trattamento: implementazione misure o consultazione preventiva

In funzione della valutazione della gravità e della probabilità per ciascun binomio minaccia-danno, si determineranno i principali danni per l'interessato e i rischi. Pertanto, si procederà alternativamente:

- con l'implementazione di misure e accorgimenti opportuni, che dovranno ridurre il rischio ad un livello contenuto;
- con la consultazione dell'autorità di controllo in caso di assenza di misure adeguate per attenuare il rischio elevato rilevato.

Implementazione delle misure e calcolo del rischio residuo

Dovrà essere valutato, a monte, il livello di adeguatezza delle misure da implementare, in termini organizzativi/operativi e tecnici, in ragione dell'efficacia di mitigare significativamente il rischio.

Individuate le misure, è necessario effettuare nuovamente la valutazione di gravità e probabilità per ciascun binomio minaccia-danno, al fine di valutare **il rischio residuo** connesso al trattamento. Qualora il giudizio della DPIA considerasse che il trattamento dei dati personali in oggetto, mediante l'implementazione delle misure adottate, conduca ad un rischio residuo per i diritti e le libertà degli interessati determinabile come corrispondente a un livello "Basso" (non elevato), si procederà alla loro implementazione.

Andrà poi monitorata l'effettiva implementazione delle misure nel rispetto della pianificazione prevista.

Consultazione preventiva dell'Autorità di controllo in assenza di misure adeguate alla mitigazione del rischio

Se non sussistano misure adeguate e si ritiene che il trattamento possa violare le previsioni del GDPR, il Titolare consulta preventivamente il Garante privacy il quale fornirà, entro un termine di otto settimane (prorogabile tenendo conto della complessità del trattamento) un parere scritto.

Nella richiesta di consultazione andranno indicate le seguenti informazioni:

- le responsabilità del Titolare del trattamento, dei contitolari del trattamento e dei responsabili del trattamento;
- le finalità e i mezzi del trattamento;
  le misure e le garanzie previste per proteggere i diritti e le libertà degli interessati a norma del GDPR; ove applicabile, i dati di contatto del DPO;
- le risultanze della DPIA.

CRITERI DI VERIFICA DELL'ADEGUATEZZA DELLA DPIA ESEGUITA	ELEMENTI UTILI ALLA VERIFICA
LA DPIA PREVEDE UNA DESCRIZIONE SISTEMATICA DEL TRATTAMENTO?	1. sono presi in considerazione natura, portata, contesto e finalità del trattamento sono descritti i dati personali, i destinatari e il periodo in cui verranno memorizzati; 2. è fornita una descrizione funzionale del trattamento; 3. sono indentificate le risorse su cui sono trattati i dati personali (hardware, software, reti, persone, mezzi di conservazione o di trasmissione cartacei) 4. sono tenuti in considerazione codici di condotta approvati
LA DPIA PREVEDE LA VALUTAZIONE DEGLI ELEMENTI DI "NECESSITÀ E PROPORZIONALITÀ"?	5. sono determinate le misure che contribuiscono alla proporzionalità e necessità del trattamento 6. sono determinate le misure che contribuiscono ai proteggere i diritti delle persone interessate
LA DPIA PREVEDE I RISCHI PER I DIRITTI E LE LIBERTÀ DELLE PERSONE E LE MODALITA' PER GESTILIRLI?	1. sono analizzate origine, natura, particolarità e gravità dei rischi, si tiene in considerazione l'aspettativa/punto di vista delle persone interessate per ciascun rischio (accesso illegittimo, modifica indesiderata, e la scomparsa dei dati) 2. sono prese in considerazione le fonti di rischio 3. sono identificati gli impatti potenziali per i diritti e le libertà delle persone in caso di accesso illegittimo, modifica indesiderata e perdita dei dati; 4. vengono identificate le minacce che potrebbero portare ad accesso illegittimo, modifica indesiderata e perdita dei dati; 5. sono stimate la probabilità e la gravità; 6. sono determinate le misure previste per il trattamento di tali rischi
DURANTE L'EFFETTUAZIONE DELLA DPIA SONO STATE COINVOLTE TUTTE LE PARTI INTERESSATE?	7. è stata richiesta la consulenza del DPO 8. si è tenuto conto del punto di vista/legittima aspettativa degli interessati o dei loro rappresentanti (es. associazione di consumatori, associazioni di categoria, albi professionali ecc).

Il Garante potrà, poi, richiedere informazioni integrative.

Si tenga presente che il GDPR prevede che la legge nazionale (italiana nel nostro caso) potrà prescrivere specifici casi in cui si renda che i Titolari consultino l'autorità di controllo, e ne ottengano l'autorizzazione preliminare, in relazione al trattamento per l'esecuzione di un **compito di interesse pubblico**, con riguardo alla protezione sociale e **alla Sanità pubblica**.

Una volta assunta la metodologia di effettuazione della valutazione di impatto, le Strutture sanitarie potranno procedere avendo margini di flessibilità quanto alla sua forma, posto che secondo l'approccio sostanziale del Regolamento- qualunque sia la sua forma- una DPIA deve essere una vera e propria valutazione dei rischi che consenta di adottare misure per affrontare tali rischi.

Oltre ai modelli di metodologie replicabili, sono stati individuati alcuni criteri per la conduzione di un "adeguata DPIA" (riportati nell'allegato 2 alle linee guida del WP art 29).
In specifici contesti è, comunque, potrebbe essere opportuno lo sviluppo di DPIA che tenga conto anche di alcuni "aspetti di settore" (es. in ambito sanitario) ove occorre attingere a conoscenze specifiche. Ciò perché la DPIA deve essere indirizzata a particolari tipi di trattamenti, di dati, di applicativi in uso, e di potenziali precise ripercussioni (si pensi quelle specifiche che attengono i pazienti).

4.2 ——— Piano di adeguamento: piano di attività e valutazione di sostenibilità

4.2.1 ——— Adozione di un piano di adeguamento

Il seguente schema sintetizza le tre fasi principali per l'adozione di un piano di adeguamento complessivo che un ente sanitario dovrebbe compiere per realizzare un programma di compliance al GDPR
Per ciascuna fase nei paragrafi che seguono si fornisce una sintesi degli obiettivi, delle azioni e dei risultati attesi.

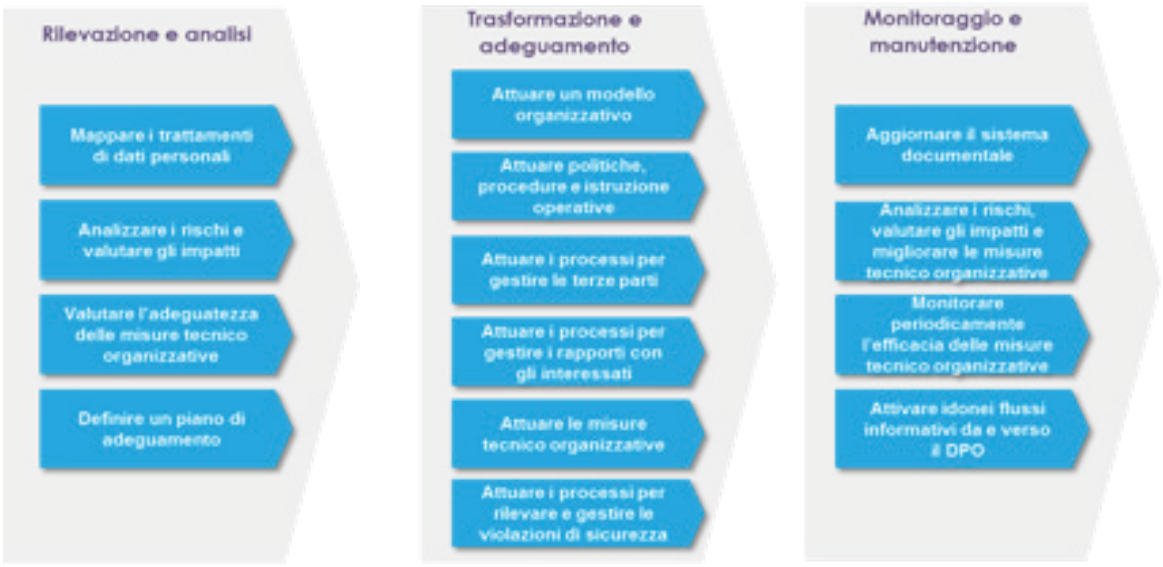


Figura: fasi principali per l'adozione di un piano di adeguamento - Fonte: Deloitte

4.2.2 ——— Rilevazione e analisi

A questa fase sono riferibili l'insieme delle azioni volte a costruire il piano complessivo di data governance.

Mappare i trattamenti di dati personali

Obiettivo dell'attività è definire e attuare la mappatura dei trattamenti dei dati personali svolti all'interno delle singole Direzioni/funzioni e predisporre il Registro dei trattamenti con le informazioni tassative previste dall'art. 30 del GDPR. Per raggiungere questo obiettivo è necessario che l'ente sanitario:

- Definisca un modello di riferimento per il registro dei trattamenti (ad es. una scheda di raccolta informazioni) secondo i requisiti declinati dall'art. 30 del GDPR
- Condivida il modello con i referenti al fine di ottimizzare le informazioni da raccogliere
- Crei il Registro dei trattamenti in un formato editabile e facilmente condivisibile (i.e. fogli Excel, DB Access, Share Point, ecc.).
- Effettui la Mappatura ex novo o proceda con l'aggiornamento dei trattamenti effettuati utilizzando il nuovo modello di riferimento

Il risultato sarà la base di un registro dei trattamenti coerente con il dettato normativo e condiviso tra i soggetti che ne dovranno curare l'alimentazione e l'aggiornamento su base periodica e che rappresenta anche la base sulla quale costruire i piani di privacy remediation più appropriati. Il tutto dovrà poi essere fatto confluire nel vero e proprio registro al fine di poter conferire il valore di forma scritta a quanto redatto, per poterlo esibire correttamente in caso di richiesta delle autorità preposte.

Analizzare i rischi e valutare gli impatti e valutare l'adeguatezza delle misure tecnico-organizzative

Obiettivo dell'attività è per ogni trattamento di dati personali effettuare una **valutazione di adeguatezza** dei presidi e delle misure in essere, che include l'analisi dei rischi tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo. Il Titolare dovrà:

- calcolare il rischio inerente quale prodotto tra le probabilità di accadimento delle minacce e i potenziali impatti per il Titolare del Trattamento e per gli Interessati
- valutare le misure di sicurezza implementate,
- calcolare il rischio residuo a valle dell'effettiva presenza delle misure
- definire adeguate misure tecnico-organizzative affinché il rischio sia classificabile come non elevato

Nel valutare l'adeguato livello di sicurezza, si deve tener conto dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata (furto) o dall'accesso, anche in modo accidentale od illegale, a dati personali trasmessi, conservati o comunque trattati» (art. 32, parag. 2)

La valutazione di adeguatezza è propedeutica alla valutazione di impatto, quando prima di procedere al trattamento il Titolare valuti che un tipo di trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche anche in base a quanto definito dal parere espresso dal GdL ex art. 29 che ha definito per ora 10 classi di trattamento per le quali è obbligatorio procedere alla valutazione d'impatto. Qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento presenta un rischio residuo non basso, il Titolare del trattamento, prima di procedere al trattamento, consulta l'autorità di controllo, al fine di individuare misure idonee per attenuare il rischio.

Piano di adeguamento

A valle delle attività di mappatura dei trattamenti, valutazione di adeguatezza e ove necessario di valutazione d'impatto, il Titolare dovrà procedere con la definizione di una road map degli interventi da attuare sotto forma di piano di adeguamento. Il piano dovrà essere strutturato per fornire le seguenti informazioni:

- Modalità di aggiornamento del Modello Organizzativo Privacy e identificazione di ruoli e responsabilità (DPO, Data Protection Committee, Data Processor, Organi di controllo, ecc)
- Gestione degli incidenti di sicurezza correlati alla perdita dei dati (c.d. Data Breach Notification)
- Gestione del rapporto con gli interessati e le terze parti.
- Individuazione delle tecnologie e delle misure tecniche da applicare sui dati personali (data deletion, Business continuity, cyber security).

4.2.3 ——— Trasformazione e adeguamento

A questa fase sono riferibili l'insieme delle azioni volte ad adeguare e/o integrare il piano complessivo di data governance

Attuare un modello organizzativo

Il Titolare dovrà definire e/o adeguare il proprio modello organizzativo privacy alla luce dell'evoluzione dei ruoli privacy e dell'introduzione della figura del DPO.

In particolare deve:

- Identificare le principali figure coinvolte nelle varie aree operative impattate da trattamenti, avuto particolare riguardo all'identificazione e successiva nomina del Data Protection Officer (DPO)
- Valutare lo stato dell'arte (as-is) della gestione delle informazioni, dei ruoli e delle responsabilità anche alla luce dell'impatto sulle informative e moduli di consenso
- Definire i flussi informativi tra le diverse figure coinvolte nel modello organizzativo di data protection & governance
- Definire le job description dei ruoli coinvolti nel modello organizzativo in ambito data protection
- Predisporre linee guida e istruzioni operative per i diversi soggetti coinvolti

Attuare politiche, procedure e linee guida

La qualità di un buon modello organizzativo per la data protection è direttamente misurabile in base alla documentazione adottata per il suo funzionamento dal Titolare. In questo senso è necessario che l'ente sanitario si doti di un robusto corredo procedurale declinato in modo tale da traguardare il principio di accountability sancito dal Regolamento.

In particolare il Titolare dovrà:

- Esplicitare in un documento di politica d'indirizzo generale l'impegno e il commitment del management aziendale sul tema della data protection e della protezione dei dati personali degli interessati (Politica aziendale sul tema della data protection)
- Redigere Linee guida che offrano una bussola ed un orientamento di alto livello per tutti coloro aziendalmente coinvolti nel trattamento dei dati personali (ad es. Manuale per l'adeguamento Privacy)
- Predisporre procedure operative che offrano ai soggetti coinvolti nel trattamento indicazioni precise su singole tematiche (modalità di gestione dei diritti degli interessati, modalità di nomina degli incaricati del trattamento, istruzioni per il trattamento dei dati nell'ambito delle attività di sperimentazione clinica, ecc.)

Attuare i processi per gestire le terze parti

Il GDPR stabilisce che nei rapporti con i fornitori e le Terze Parti, occorre garantire un efficace governo dei trattamenti affidati all'esterno al fine di minimizzare i rischi secondo un giusto bilanciamento tenuto conto dello stato dell'arte e dei costi di attuazione delle misure di prevenzione rispetto ai rischi. Il Titolare dovrà quindi:
Individuare gli scenari operativi e dei processi per la gestione degli eventuali impatti sulla filiera fornitura
Definire gli schemi contrattuali appropriati per la messa in opera degli scenari operativi
Definire le istruzioni operative per i Responsabili del trattamento in relazione ai principi del GDPR e al sistema di Data Protection identificando gli impatti organizzativi ed operativi

Attuare i processi per gestire i rapporti con gli interessati

Il GDPR pone particolare enfasi alle modalità attraverso le quali gli interessati devono poter esercitare i propri diritti: in modo agevole, secondo modalità tassative, in maniera gratuita, inviando richieste per via elettronica, con risposte che siano formulate senza ingiustificato ritardo e, in caso di rifiuto ottenendo la motivazione. Inoltre il diritto alla portabilità conferisce all'interessato il diritto di trasferire i propri dati tra diversi sistemi elettronici, in modo agevole.
Per garantire l'esercizio dei diritti, il Titolare sarà chiamato ad effettuare le seguenti azioni:

- Definire delle linee guida i per la gestione dei diritti degli interessati del trattamento, applicabili a tutti i trattamenti aziendali
- Individuare le modalità per la facilitazione dell'esercizio dei diritti da parte degli interessati (es. riscontro all'accesso, opposizione al direct marketing, rettificazione, portabilità, ecc.)
- Definire le istruzioni operative di dettaglio specifiche per classi di incaricati o addetti al trattamento
- Definire gli schemi e modelli per standardizzare la risposta agli interessati del trattamento e definizione delle eventuali specifiche funzionali per l'automatizzazione del processo di gestione delle richieste degli interessati
- Definire le modalità operative per il trasferimento dei dati personali all'interessato o direttamente ad altri titolari del trattamento
- Identificare e valutare gli impatti a livello organizzativo ed operativo a seguito della definizione delle modalità operative

Attuare le misure tecnico organizzative

Il Titolare del trattamento è chiamato a mettere in atto misure tecniche e organizzative adeguate per garantire che siano trattati solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento di una persona fisica, ovvero in modalità totalmente automatizzata.
Questo comporta che la combinazione tra principio di accountability e protezione dei dati fin dalla progettazione ("by design") e per impostazione predefinita ("by default"), attribuisca la **responsabilità al Titolare del trattamento** riguardo all'adozione di policy interne e all'implementazione di misure appropriate per assicurare e dimostrare le compliance con la normativa.

In particolare il Titolare deve:

- Formalizzare tramite linee guide operative il principio per cui solo i dati personali necessari per il perseguimento di una determinata finalità sono raccolti ed utilizzati, anche in termini di ambito del trattamento, periodo di conservazione, e accessibilità
- Definire un modello organizzativo che possa applicarsi a i nuovi trattamenti di dati personali, con il coinvolgimento del DPO non solo nelle fasi iniziali del trattamento, per la valutazione degli aspetti connessi alla minimizzazione
- Definire un modello di riferimento che consenta la gestione, by default, di tutti gli aspetti che garantiscono la legittimità del trattamento
- Individuare i criteri operativi per la minimizzazione dei dati personali sia in fase di raccolta sia in fase di utilizzo dei dati
- Definire la correlazione dei dati e della interconnessione dei dati con altre base dati

Attuare i processi per rilevare e gestire le violazioni di sicurezza

Il Titolare deve necessariamente dotarsi di un Piano completo di Data Breach Management che non sia limitato alla sola fase di violazione e successiva gestione delle violazioni ma deve essere strutturato come un processo che partendo dal momento della raccolta dei dati personali, passi attraverso la fase di mappatura, prosegua tramite la verifica dell'adozione di misure di sicurezza adeguate e si concluda con l'eventuale notifica all'autorità Garante e/o con la comunicazione agli interessati, cui seguirà una necessaria fase di contenimento e rimedio.

In questo senso il Titolare deve, a valle di una verifica delle ipotesi nelle quali si potrebbe generare una violazione di dati personali, procedere definendo una procedura per il Data Breach Management che sia coerente con il modello organizzativo privacy adottato e che definisca i ruoli, le responsabilità, i presidi di controllo e le modalità per la comunicazione delle violazioni sui dati personali (tempistiche, modalità, istruzioni operative, etc.)

4.2.4 ——— Monitoraggio e manutenzione

A questa fase, sono riferibili l'insieme delle azioni volte a monitorare nel continuo il piano complessivo di data governance affinché mantenga le caratteristiche di efficacia ed efficienza.

Aggiornare il sistema documentale

Il Titolare è tenuto a mantenere nel tempo l'insieme delle procedure poste a presidio del proprio sistema di data governance verificando l'efficacia dei presidi anche in base all'evoluzione normativa e svolgendo periodiche azioni di analisi e controllo sulle proprie basi dati da un punto di vista della mappatura dei trattamenti.

Analizzare i rischi, valutare gli impatti e migliorare le misure di sicurezza

Il Titolare, sulla base dei risultati della periodica mappatura dei trattamenti, è tenuto a effettuare sui nuovi trattamenti sia la valutazione di adeguatezza delle misure di sicurezza sia, eventualmente, a svolgere la valutazione di impatto. A valle di queste attività, correlate ma indipendenti, il Titolare dovrà implementare un piano di remediation per migliorare le misure di sicurezza precedentemente adottate secondo lo schema del continuous improvement

Monitorare l'efficacia delle misure di sicurezza

Il Titolare deve monitorare nel continuo l'efficacia delle misure di sicurezza adottate dotandosi di strumenti per la verifica ed il controllo periodico quali check list o piani di audit.

5.1 —— Cosa intendiamo per Big Data

In ambito sanitario primaria importanza riveste la realizzazione di un modello di governo e gestione della data protection.

Per definire in maniera appropriata il modello organizzativo, è importante partire dal contesto di riferimento in base al quale è possibile definire una struttura che precisi sia i ruoli e le responsabilità con riferimento a quanto previsto dalla normativa, sia le entità organizzative che possono svolgere un ruolo di coordinamento a presidio di attività operative che le imprese sanitarie possono valutare di introdurre al dine di fornire maggiori garanzie in ordine all'adeguatezza del proprio sistema di data governance e nella prospettiva di dimostrare l'accountability (es. Comitato Data Protection, Chief Privacy Officer, Data Manager, etc).

Il Regolamento (UE) 2016/679 precisa dei ruoli già esistenti nella prassi, come il ConTitolare, e introduce il nuovo ruolo del DPO, introdotto con il GDPR, storicamente già citato nella direttiva madre, ovvero la 95/46[14], recepito da alcune legislazioni europee, e che rappresenta un professionista (sia esso soggetto interno o esterno) con competenze normative, informatiche, gestionali, di risk management e di analisi dei processi etc. La sua responsabilità principale è quella di osservare, valutare e organizzare la gestione del trattamento di dati personali (e dunque la loro protezione) all'interno di un'azienda (sia essa pubblica che privata), affinché questi siano trattati nel rispetto delle normative privacy europee e nazionali. Secondo quanto indicato dal GDPR, il DPO è una figura di vigilanza e non di garanzia, non deve pertanto garantire la conformità alle prescrizioni del Regolamento, ma vigilare sul loro effettivo funzionamento.

5.1.1 —— Schema organizzativo per la Data Protection

Il seguente schema sintetizza una possibile vista organizzativa per la Data Protection Governance coerente con le indicazioni del GDPR e in grado di garantire un elevato livello di "performance privacy" nella gestione, nel continuo, degli obblighi di tutela dei diritti e della dignità dell'interessato tipici di un'entità che opera in un ambiente di tipo sanitario.

Figura 1: Schema del modello organizzativo Data Protection - Fonte: Deloitte

14. http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046&from=IT

Il modello di data protection governance proposto si sviluppa a partire da un ***sistema di deleghe*** che per essere efficace deve essere, anzitutto, effettivo. La letteratura in materia, infatti, ha da tempo riconosciuto come il semplice atto del nominare qualcuno (ad es. il Responsabile del trattamento interno) in modo surrettizio e senza la dotazione dei necessari strumenti operativi non scarica il Titolare delle responsabilità in caso di danno causato per l'illecito (o illegittimo) trattamento di dati personali.
La delega di funzioni, al pari di quanto richiesto da altra normativa cogente (si pensi alla nomina del Delegato del Titolare o del RSPP prevista dal D. Lgs. 81/08 ovvero del Dirigente Preposto indicato dalla Legge 262/05), deve essere effettuata tenendo conto dei seguenti aspetti: forma, specificità della delega, accettazione, effettività, competenza tecnica del delegato, non ingerenza del delegante, vigilanza del delegante, dimensioni dell'organizzazione.
Il modello è suddiviso in 2 parti, connesse e funzionali, che a fronte di un Livello di Governo, cui sono demandate le decisioni di indirizzo strategico, vede un Livello di Linea in cui si concentrano le risorse che, operativamente, si trovano a contatto quotidiano con i soggetti interessati dal trattamento.
Di seguito, per ciascuna figura prevista nel modello, si fornisce un inquadramento esplicativo di ruoli responsabilità e delle principali mansioni che dovrebbe ricoprire.

- **Titolare del trattamento**. È la persona giuridica rappresentata dal proprio Legale Rappresentante pro tempore. Al Titolare competono, anche unitamente ad altro Titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza. Il Titolare, anche attraverso i suoi organismi di rappresentanza giuridica (CdA) emana un atto regolamentare per creare il Comitato Data Protection, provvedendo alla nomina delle figure che lo compongono: Presidente, DPO, CISO, Responsabile Sicurezza Fisica. Il Titolare delega il Presidente nell'esercizio del ruolo di coordinamento del Comitato stesso e gestisce, in collaborazione con il Comitato, la verifica dell'operato dei Responsabili del trattamento coinvolti ed eventuali richieste provenienti dal Garante per la protezione dei dati personali.
- **Comitato Data Protection**. È l'organismo cui sono demandate le decisioni di tipo strategico e di indirizzo in materia di protezione dei dati personali. Pur se non direttamente previsto dal GDPR assolve funzioni di coordinamento e analisi interna compatibili con il più ampio principio di accountability previsto dal GDPR. La struttura del Comitato, è composta da membri permanenti che occupano ruoli chiave all'interno delle rispettive realtà e hanno competenze tali da garantire presidio normativo, tecnico e fisico. A copertura dei tre ambiti possono essere identificati il CIO (Chief Information Officer) o suo delegato (ad es *Chief Security Information Officer.*), il DPO (*Data Protection Officer;*) il Risk Manager, il *Responsabile della Sicurezza fisica* (individuato nel Responsabile dell'Ufficio Tecnico o laddove esistente nel Safety & Facility Management). Tra i membri permanenti possono essere inseriti anche il Direttore Sanitario nonché altri *Responsabili di Direzione* che occupano ruoli chiave all'interno delle rispettive realtà che trattano massivamente dati personali di pazienti e dipendenti (ad es. Direzioni Ricerca, HR, URP).
- **Data Protection Officer (DPO)**. Attesa la sua obbligatorietà in ambito sanitario può operare indistintamente all'interno o all'esterno di un Comitato Data Protection. Il DPO svolge un ruolo centrale nel sistema data protection e di tutela dei diritti e delle libertà fondamentali degli interessati

Figura 2: Interrelazioni del DPO con gli altri organi di controllo e governo aziendale - Fonte: Deloitte

Il DPO interagisce con i vari soggetti per l'emanazione di politiche e linee guida e promuove l'attuazione e l'applicazione delle politiche privacy all'interno azienda sanitaria. Verifica che sia applicato quanto richiesto dalla normativa con particolare riguardo ai requisiti concernenti la protezione dei dati in termini di informazione all'interessato e gestione dell'esercizio dei propri diritti.Inoltre tra le sue responsabilità ci sono compiti di indirizzo, coordinamento e verifica delle attività di adempimento alla normativa Privacy e di controllo sulle eventuali violazioni e/o Data Breach in termini di documentazione, notificazione al Garante e comunicazione alle parti interessate (qualora coinvolte). Inoltre può assumere il compito di punto di contatto per il Garante Privacy nel caso di verifiche ispettive e verso gli Interessati per l'esercizio dei loro diritti o per fornire informazioni e fornisce, se richiesto, pareri ed indicazioni in merito alla conduzione, valutazione e follow up conseguenza di valutazione d'impatto (o DPIA).
Il DPO potrebbe dotarsi del "DPO Chart" che può essere utilizzato per codificare i meccanismi di funzionamento in ordine alle attività di vigilanza e di riporto al Titolare del trattamento e agli organi di controllo e governo.

- **Responsabili del trattamento**. Pur se dalla lettura del GDPR potrebbero sussistere dei dubbi circa l'obbligatorietà di prevederne la figura e la nomina, se ne consiglia e caldeggia l'adozione come necessaria in quanto rappresenta il soggetto che, per esigenze organizzative, può intervenire nel meccanismo di gestione della privacy essendo spesso identificato con una figura apicale con forte potere decisionale (ad es. Responsabili di Direzione Ricerca, Clinica, Personale, Amministrazione, Marketing). il Responsabile esegue i suoi compiti sulla base delle istruzioni scritte ricevute e si interfaccia con i DPM, Data Processing Manager, personale nominato dallo stesso quale riferimento operativo per le attività day-by-day
- **Data Processing Manager (DPM)**. Sono figure, facoltative e non previste dal GDPR, che possono essere designate dai Responsabili di Trattamento quali focal point per la gestione operativa delle attività connesse al trattamento dei dati personali, in realtà particolarmente complesse e articolare sia da un punto di vista geografico che dei tipi di servizi resi sul territorio. I DPM possono essere tutti coloro che hanno un ruolo di Responsabile di Servizio e sono identificati dal Responsabile, per specifica Area di competenza. Il Responsabile delega la gestione delle operazioni di trattamento dei dati personali

mantenendo potere decisionale e fornendo linee guida di alto livello e indirizzamenti sulle azioni da adottare a fronte di segnalazioni dei DPM. Il Gruppo riduce il rischio di disomogeneità interpretative della norma, applicando la stessa in maniera puntuale per le varie Aree.

- **Amministratori di Sistema**. Fatte salve le realtà che non hanno un proprio sistema informatico è assolutamente necessario prevedere la nomina dei soggetti preposti alla gestione e alla manutenzione di un impianto di elaborazione dati o di sue componenti. il Provvedimento del Garante Privacy del 27 novembre 2008 (*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*) considera anche altre figure quali: gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi che vanno debitamente nominate e periodicamente controllate. Stanti le peculiarità tecniche, l'Amministratore di Sistema ricopre un ruolo estremamente delicato: progetta, sviluppa e gestisce l'infrastruttura di rete, i server, il software ed i servizi applicativi di base occupandosi spesso della sicurezza e della protezione dei dati e delle risorse. Inoltre fornisce supporto tecnico (help desk) e informatico su software e hardware. Quando necessario ricopre un ruolo proattivo nell'ambito delle notificazioni di violazioni di sicurezza e data breaches, notificando al CISO (o al DPO) eventuali anomalie riscontrate su malfunzionamenti o rischi di sicurezza. Risponde delle attività svolte e delle conseguenze derivanti da un malfunzionamento della rete e supporta Responsabili del Trattamento e Incaricati per gli aspetti di tipo tecnico informatico nelle normali attività operative.
- **Incaricati del trattamento**. Il GDPR seppur non esplicitamente li cita come quei soggetti che operano quali "persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del Titolare o del responsabile" (art. 4, n. 10, del GDPR). Sulla nomina scritta non paiono sussistere dubbi atteso che l'incaricato è chiamato a ricoprire un ruolo operativo dovendo collaborare con il proprio Responsabile e utilizzando dati solo per gli scopi istituzionali, nello spirito della legge e secondo le istruzioni scritte che ha ricevuto. Nello svolgimento delle proprie mansioni, rispetta il segreto di ufficio e professionale, oltre che i requisiti di riservatezza e sicurezza durante l'uso dei dati personali.

5.2 ——— Titotale e conTitolare

Il tema della Co-titolarietà dei dati (art.26) è un tema particolarmente interessante in Sanità in quanto semplifica il quadro normativo rispetto a trattamenti che possono esser svolti da più titolari su uno specifico processo di cura. Ci si riferisce prevalentemente al tema dell'utilizzo di nuovi modelli organizzativi, di tipo trasversale (ospedale-territorio-domicilio), denominati PDTA, per il trattamento della cronicità. Con frequenza questi nuovi modelli organizzativi comportano un trattamento svolto da più professionisti in luoghi e tempi diversi ma anche appartenenti a legal entity diverse.

Riprendendo i contenuti del documento AISIS su PDTA e Data protection[15], un "PDTA può essere configurato a tutti gli effetti come un trattamento sanitario di durata definita, effettuato da una entità virtuale costituita da una pluralità di soggetti legati da un contratto specifico che ne definisce ruoli e responsabilità.

La definizione di co-titolarità presente nel GDPR all'art. 24 si attaglia esattamente al PDTA così descritto e consente di impostare sia l'informativa che il consenso in modo conseguente: un'unica informativa ed un solo consenso che riguardano l'intero PDTA.

15. Aisis, PDTA e Data Protection: normativa, organizzazione e tecnologia, ***2016***

Dalla definizione di cui sopra discende anche che il paziente, concedendo il proprio consenso al PDTA, acconsente al fatto che i dati detenuti dai singoli co-titolari vengano fra essi condivisi e resi accessibili ai fini della gestione del PDTA.
Il PDTA, dunque, è equiparabile ad un ricovero ospedaliero con la relativa cartella clinica elettronica: di conseguenza tutti i dati facenti parte del PDTA sono consultabili dagli attori coinvolti nella gestione del PDTA per come questa si svilupperà in base alle esigenze cliniche e per la sola sua durata.
Di fatto quindi, così come la cartella clinica è l'insieme dei dati sanitari che afferiscono ad un unico episodio di cura, accessibili quindi a tutti i professionisti coinvolti nella cura del paziente fintanto che il paziente è "in cura", analogamente un PDTA raccoglie dati nell'ambito di un intervallo di tempo all'interno del quale diversi professionisti operano in modo contemporaneo o sequenziale (anche non continuativo) per curare il paziente in un unico percorso che ha un momento (evento) di inizio e un momento (evento) di chiusura. Fra questi due istanti di tempo (inizio e fine) il paziente è "in cura" nel PDTA e pertanto i dati del PDTA sono accessibili da parte di tutti i professionisti coinvolti in questo specifico processo di cura (PDTA).

In tale contesto si evidenzia che il PDTA, a differenza del ricovero, tende ad essere una "vista aggregata" di dati sociosanitari, alcuni di essi già esistenti nei Dossier dei diversi co-titolari, ovviamente nel rispetto dei consensi espressi dall'assistito in merito ai Dossier dei singoli co-titolari e degli eventuali oscuramenti sui dati in essi contenuti. Non si tratta in effetti di creare un ulteriore "dossier fisico" o una sorta di "cartella clinica di PDTA" ma di realizzare una restituzione "intelligente" di informazioni disponibili in sistemi già in uso (cartelle cliniche e infermieristiche, cartelle dei MMG, cartelle ambulatoriali, Dossier...) aggregando le informazioni sui "workflow dei PDTA" attraverso l'utilizzo di motori di integrazione (Enterprise Service Bus) ampiamente utilizzati in altri settori merceologici, consentendo così l'accesso anche ad informazioni non prodotte all'interno del PDTA che potessero risultare utili per ridurre la necessità di ulteriori esami o trattamenti previsti dal protocollo ma già effettuati per altre ragioni.

L'insieme dei dati necessari per la gestione del PDTA si costituisce quindi solo in modo virtuale e la condivisione/consultazione dei dati, che viene consentita ai co-titolari, viene dichiarata nello specifico consenso richiesto al paziente nella fase di "accettazione all'arruolamento" nel PDTA.

Laddove tale scelta non fosse possibile sotto il profilo tecnologico e si dovesse rendere necessaria la costituzione "fisica" di un Dossier a supporto del PDTA, sarà necessario dichiarare tale modalità operativa nell'informativa ed acquisire uno specifico consenso alla costituzione di uno specifico Dossier del PDTA stesso."

Il GDPR prevede la possibilità di contrattualizzare la cotitolarietà, definendo le reciproche responsabilità e dandone chiara e trasparente informazione ai cittadini (come normato agli art.13 e 14).

5.2.1 —— Il Titolare

Il **Titolare del trattamento** è definito nell'art. 4 del Regolamento come "l***a persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali***", e *"quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il Titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri".*

Il Titolare è il soggetto su cui grava la responsabilità generale del trattamento, che deve adempiere alle pre-

scrizioni contenute nelle varie disposizioni del Regolamento e che deve **essere in grado di dimostrare** che il trattamento dei dati personali è effettuato conformemente al Regolamento secondo il principio di responsabilità e l'efficacia delle misure adottate ("***accountability***")[16]

Viene introdotta, infatti, un'elevata responsabilizzazione del Titolare che deve avere un approccio proattivo e l'obbligo di una costante valutazione del contesto e del settore in cui opera per poter garantire la costante conformità delle operazioni di trattamento.

Gli artt. 24 e 25 del Regolamento individuano gli obblighi generali in capo al Titolare del trattamento, mentre obblighi specifici sono contenuti in varie altre disposizioni analizzate nei diversi capitoli del presente testo.

Il Titolare può dimostrare il rispetto degli obblighi a suo carico anche attraverso l'adesione a codici di condotta o a meccanismi di certificazione di cui agli artt. 40-42 del Regolamento[17].

In particolare, fra gli obblighi generali del Titolare è prevista l'adozione di **misure tecniche ed organizzative adeguate**[18]:

- per **garantire, ed essere al contempo in grado di dimostrare, che il trattamento è effettuato in conformità al Regolamento e** che includono l'attuazione di **adeguate politiche** in materia di protezione dei dati personali (art. 24), ad esempio per essere in grado di effettuate una **notificazione della violazione** dei dati nel rispetto delle tempistiche previste (art. 33) e dare un **riscontro tempestivo all'interessato che eserciti i propri diritti** (artt. 12 e ss.).
- per **proteggere i dati fin dalla fase di ideazione e progettazione** del trattamento o di un sistema e nel corso del trattamento stesso (c.d. "*Privacy by Design*"), ad esempio mediante tecniche di pseudoanonimizzazione (art. 25);
- per garantire che siano **trattati, per impostazione predefinita, solo i dati personali necessari per ogni singola finalità del trattamento** (c.d. "*Privacy by Default*") rendendo inaccessibili i dati personali ad un numero indefinito di persone fisiche senza l'intervento della persona fisica, e ciò con riferimento alla quantità dei dati personali raccolti, alla portata del trattamento, al periodo di conservazione ed all'accessibilità (art. 25);

Nell'individuazione delle misure tecniche ed organizzative adeguate, **il Titolare deve tener conto dei seguenti elementi:**

- lo **stato dell'arte ed i costi di attuazione** limitatamente all'approccio di *Privacy by Design*;
- la **natura del trattamento**;
- l'**ambito di applicazione**;
- il **contesto**;
- le **finalità** del trattamento;
- i **rischi aventi probabilità e gravità diverse** per i diritti e le libertà delle persone fisiche.

16. Vedi supra Capitolo 5.
17. Vedi infra Capitolo 16.
18. Si rammenta che il Dipartimento della Funzione Pubblica aveva già adottato una Direttiva in data 9 febbraio 2005 do le pubbliche amministrazioni ad implementare, fra l'altro, misure organizzative in conformità al D.Lgs./2003.

Relativamente a tale ultimo elemento, il Considerando n. 75 del Regolamento precisa che i **rischi per i diritti e le libertà delle persone fisiche** aventi probabilità e gravità diverse "**possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico materiale o immateriale**" ed indica in particolare i seguenti:

- se il trattamento può comportare **discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perd ta di riservate za dei dati personali protetti da segreto professionale, decifratura non autorizzata** della pseudonimizzazione**, o qualsiasi altro danno** economico o sociale significativo;
- se gli interessati rischiano di essere **privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo** sui dati personali che li riguardano;
- **se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza;**
- in caso di **valutazione di aspetti personali**, in particolare mediante l'analisi o la previsione di 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, al fine di creare o utilizzare profili personali;
- **se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori;**
- **se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati.**

La probabilità e gravità del rischio devono essere determinati dal Titolare tenendo conto degli stessi elementi considerati per l'individuazione delle misure tecniche ed organizzative adeguate[19].

Con riferimento alle **misure in grado di soddisfare i principi della *Privacy by Design e by Default***, che dovrebbero essere presi in considerazione **anche nell'ambito degli appalti pubblici**, sono di ausilio le indicazioni contenute nel Considerando 78 del Regolamento che indica a titolo esemplificativo:

- la **riduzione al minimo del trattamento** dei dati personali;
- l'adozione di **tecniche di pseudonimizzazione**;
- la **trasparenza** per quanto riguarda le funzioni e il trattamento di dati personali;
- la **facoltà dell'interessato di controllare** il trattamento dei dati **e del Titolare** del trattamento di **creare e migliorare caratteristiche di sicurezza**[20].

Lo stesso 78 incoraggia, peraltro, i produttori di prodotti, servizi ed applicazioni a tenere conto del diritto alla protezione dei dati già durante la fase di sviluppo e progettazione per consentire ai Titolari ed ai Responsabili di adempiere ai propri obblighi.

19. Vedi Considerando n. 76
20. Vedi il Considerando 78 incoraggia i produttori di prodotti, servizi ed applicazioni a tenere conto del diritto alla protezione dei dati in fase di sviluppo e progettazione per consentire ai titolari ed ai responsabili di adempiere ai propri obblighi.

5.2.2 ——— Il conTitolare

L'art. 26 del Regolamento disciplina espressamente l'ipotesi di **contititolarità** del trattamento, situazione che si ravvisa q**uando due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento**[21].

In tal caso, i contitolari hanno l'**obbligo di determinare in modo trasparente e mediante uno *specifico accordo interno*, le rispettive responsabilità** in merito all'osservanza degli obblighi derivanti dal Regolamento, salvo il caso in cui le rispettive responsabilità siano già determinate da una norma di legge europea o di uno Stato membro.

Un soggetto pubblico, così qualsiasi altro Titolare del trattamento, che riveste il ruolo di "conTitolare" del trattamento deve, pertanto, verificare se, anzitutto, esiste una norma di legge che determini le responsabilità di ciascun conTitolare e, in difetto, deve provvedere a redigere uno specifico **accordo interno** con l'altro conTitolare che deve avere il seguente **contenuto minimo**:

- deve riflettere adeguatamente i rispettivi **ruoli e i rapporti dei contitolari con gli interessati**;
- deve indicare le **responsabilità dei contitolari** con riferimento all'esercizio dei diritti dell'interessato e all'obbligo di informativa all'interessato;
- può designare un **punto di contatto per gli interessati**.

Il contenuto essenziale dell'accordo è, inoltre, **messo a disposizione dell'interessato**.

In ogni caso, l'**accordo** interno fra i contitolari **non pregiudica i diritti dell'interessato** il quale, indipendentemente dalle disposizioni di tale accordo, può esercitare i propri diritti nei confronti di e contro ciascun Titolare del trattamento.

5.3 ——— Nomina dei responsabili

5.3.1 ——— Riferimento Normativo

Articolo 28 GDPR Responsabile del trattamento

1. Qualora un trattamento debba essere effettuato per conto del Titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.

2. Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta,

21. La contitolarità del trattamento è una situazione già prevista nella legislazione vigente. L'art. 4, comma 1, lett. f), del D.Lgs. 196/2003 nella definizione di "Titolare" indica, infatti, la possibilità che le decisioni in merito alle à e modalità del trattamento ed agli strumenti utilizzati competono al Titolare anche unitamente ad altro Titolare

specifica o generale, del Titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il Titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al Titolare del trattamento l'opportunità di opporsi a tali modifiche.

3. I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al Titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del Titolare del trattamento.

Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento:

a) tratti i dati personali soltanto su istruzione documentata del Titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento informa il Titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;

b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;

c) adotti tutte le misure richieste ai sensi dell'articolo 32;

d) rispetti le condizioni di cui ai paragrafi 2 e 4 per ricorrere a un altro responsabile del trattamento;

e) tenendo conto della natura del trattamento, assista il Titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del Titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III;

f) assista il Titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;

g) su scelta del Titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati; e

h) metta a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal Titolare del trattamento o da un altro soggetto da questi incaricato.

Con riguardo alla lettera h) del primo comma, il responsabile del trattamento informa immediatamente il Titolare del trattamento qualora, a suo parere, un'istruzione violi il presente regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.

4. Quando un responsabile del trattamento ricorre a un altro responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del Titolare del trattamento, su tale altro responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione

o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il Titolare del trattamento e il responsabile del trattamento di cui al paragrafo 3, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento. Qualora l'altro responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile iniziale conserva nei confronti del Titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile.

5. L'adesione da parte del responsabile del trattamento a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare le garanzie sufficienti di cui ai paragrafi 1 e 4 del presente articolo.

6. Fatto salvo un contratto individuale tra il Titolare del trattamento e il responsabile del trattamento, il contratto o altro atto giuridico di cui ai paragrafi 3 e 4 del presente articolo può basarsi, in tutto o in parte, su clausole contrattuali tipo di cui ai paragrafi 7 e 8 del presente articolo, anche laddove siano parte di una certificazione concessa al Titolare del trattamento o al responsabile del trattamento ai sensi degli articoli 42 e 43.

7. La Commissione può stabilire clausole contrattuali tipo per le materie di cui ai paragrafi 3 e 4 del presente articolo e secondo la procedura d'esame di cui all'articolo 93, paragrafo 2.

8. Un'autorità di controllo può adottare clausole contrattuali tipo per le materie di cui ai paragrafi 3 e 4 del presente articolo in conformità del meccanismo di coerenza di cui all'articolo 63.

9. Il contratto o altro atto giuridico di cui ai paragrafi 3 e 4 è stipulato in forma scritta, anche in formato elettronico.

10. Fatti salvi gli articoli 82, 83 e 84, se un responsabile del trattamento viola il presente regolamento, determinando le finalità e i mezzi del trattamento, è considerato un Titolare del trattamento in questione.

5.3.2 ——— La scelta del Responsabile

Il Responsabile del trattamento ovvero la persona fisica o giuridica che tratta i dati per conto del Titolare, deve avere competenza, professionalità specifica ed approfondita conoscenza della materia relativa alla protezione e sicurezza dei dati con particolare riferimento alle norme del GDPR. Solo con tali capacità potrà essere in grado di presentare "garanzie sufficienti" per mettere in atto misure tecniche ed organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'interessato. E tali garanzie potranno essere "dimostrate" in virtù del combinato disposto della lett. h) del terzo comma e del quinto comma dell'art. 28, anche con l'adesione ad un codice di condotta approvato (ex art. 40) o ad un meccanismo di certificazione (ex art. 42).

In attesa che vengano approvati dei codici di condotta e che ci siano delle imprese che vi aderiscono o vengano definiti requisiti aggiuntivi a quelli già esistenti[22] ai fini dell'accreditamento degli organismi di certificazione, il Titolare del trattamento dovrebbe selezionare il Responsabile a cui affidare il trattamento dei propri dati richiedendo qualsiasi elemento - da valutare, allo stato attuale, anche con un certo grado di discrezionalità - a "garanzia" della compliance al GDPR o dell'esistenza di un concreto processo di adeguamento in atto. A titolo meramente esemplificativo, potrebbe essere richiesto di aver già provveduto ad individuare la figura del DPO, anche laddove non obbligatorio, o l'aver già istituito un registro dei trattamenti (e in tal caso, dando evidenza delle modalità di redazione, aggiornamento, ecc), o l'aver adottato policy per garantire che gli incaricati siano obbligati alla riservatezza o per soddisfare eventuali richieste di esercizio dei diritti degli interessati, per la data retention o ancora per il data breach. Sulla base della tipologia del trattamento e della natura dei dati trattati, il Titolare potrebbe inoltre esigere che siano state già implementate determinate misure di sicurezza, tecniche o organizzative, valutate adeguate per garantire che il trattamento sia conforme al GDPR.

5.3.3 —— Il rapporto con il Titolare e le attività del Responsabile

Il legislatore europeo ha posto particolare attenzione al rapporto giuridico che lega il Responsabile del trattamento al Titolare con il comma 3 dell'art. 28 prevedendo, a differenza della precedente prescrizione normativa europea e nazionale del codice privacy, che il contratto (o qualsiasi altro atto giuridico scritto che lega i due soggetti) abbia, inderogabilmente, alcuni contenuti minimi (la natura, le caratteristiche, la finalità e la durata del/dei trattamento/i, i tipi di dati trattati, le categorie di interessati coinvolti, gli obblighi e i diritti del Titolare) e preveda almeno quanto dettagliato dalla lett. a) alla lett. h) del terzo comma.

Come si evince dalla lettura di questo comma, il compito del Responsabile del trattamento consiste sostanzialmente nel coadiuvare ed assistere il Titolare in tutte le attività finalizzate a garantire il rispetto del GDPR, ed in particolare:

- nei limiti delle istruzioni documentate fornite dal Titolare, svolgere le attività di trattamento dati adottando le misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio (art. 28 c. 3 lett. a e c)
- garantire che le persone fisiche che di fatto dovranno operare sui dati siano non solo autorizzate in modo specifico ma si siano impegnati alla riservatezza o abbiano un obbligo legale in tal senso; ciò presuppone che il precedente atto di nomina ad incaricato evolva verso un vero e proprio NDA (art. 28 c. 3 lett. b);
- collaborare con il Titolare nel garantire l'esercizio dei diritti degli interessati di cui agli artt. da 12 a 22 e il rispetto degli obblighi in materia di sicurezza del trattamento, data breach, valutazione d'impatto sulla protezione dei dati e consultazione preventiva (art. 28 c. 3 lett. e ed f);
- mettere a disposizione del Titolare tutte le informazioni necessarie per dare evidenza del rispetto degli obblighi previsti dall'art. 28 consentendo attività di ispezione, audit o revisione ed informandolo qualora le istruzioni fornitegli violino le norme in materia di protezione dei dati (art. 28 c. 3 lett. h)
- rispettare le condizioni prescritte per ricorrere ad altro responsabile (art. 28 c. 3 lett. d);
- restituire o cancellare i dati del Titolare al termine del trattamento affidatogli (art. 28 c. 3 lett. g).

22. http://www.accredia.it/UploadDocs/7180_DC2017SSV207.pdf

Ma anche:

- coinvolgere tempestivamente ed adeguatamente il DPO (laddove previsto) in tutte le questioni riguardanti la protezione dei dati, fornendogli le risorse necessarie per assolvere i suoi compiti e accedere ai dati e ai trattamenti e mantenere la sua conoscenza specialistica pur senza fornire istruzioni per quanto riguarda l'esecuzione dei suoi compiti (art. 38 c.1, 2 e 3)
- collaborare con l'Autorità di Controllo (art. 31 e 58) e con gli organismi di certificazione (art. 42.6), laddove necessario.

È importante che la determinazione dettagliata dei compiti e delle responsabilità assegnate al Responsabile sia formalizzata precedentemente (o contestualmente) all'inizio di qualsiasi attività di trattamento.

In futuro, potranno essere di supporto eventuali clausole contrattuali "tipo" che potrebbero essere emanate dalla Commissione Europea o dalle singole Autorità di Controllo competenti in conformità ai meccanismi di coerenza previsti all'art. 63 del GDPR.

5.3.4 ——— Le responsabilità

Al fine di delimitare le responsabilità di tale figura soggettiva e differenziarle da quelle del Titolare, è necessario che i compiti e le attività assegnate, siano quanto più dettagliate nelle "istruzioni" che devono essere formalizzate fra il Titolare e il Responsabile.

Ciò al fine di delimitare anche l'eventuale danno materiale o immateriale da risarcire causato da una violazione del GDPR: ai sensi dell'art. 82 comma 2 infatti, mentre il Titolare risponde del danno cagionato dal suo trattamento che in qualunque modo violi il GDPR, il Responsabile del trattamento risponde per il danno causato dal trattamento, soltanto al verificarsi di una delle due condizioni seguenti:

- se non ha adempiuto gli obblighi specifici previsti dal GDPR per tale figura soggettiva
- se ha agito in modo difforme o contrario rispetto alle istruzioni fornite dal Titolare

Solo in tal caso, si configura una "responsabilità solidale" con il Titolare il quale, potrà avere azione di regresso nei confronti del Responsabile (o viceversa) se le "istruzioni" che sono state formalizzate sono definite con rigore.

È inoltre fondamentale che il Responsabile non decida - *de iure* nell'atto formale ma anche *de facto* nell'esercizio delle sue attività - le finalità e i mezzi del trattamento di esclusiva competenza del Titolare, in quanto, oltre a dover risarcire i danni in caso di violazione del GDPR e di essere sanzionato dall'Autorità di Controllo, viene considerato a tutti gli effetti anch'egli un Titolare del trattamento con le responsabilità - più ampie rispetto a quelle di un Responsabile - tipiche di tale figura soggettiva.

5.3.5 ——— La filiera dei sub-Responsabili

Quale novità del GDPR, se il Responsabile non svolge *in toto* i compiti assegnati dal Titolare, può affidarli ad altri responsabili previa autorizzazione scritta del Titolare del trattamento, il quale, con un certo grado di discrezionalità, può acconsentire o negare tale eventualità, oppure intervenire per chiedere delle modifiche all'affidamento. Tale autorizzazione può essere "specifica" sul singolo caso o attività delegata, o "generale", che consente al Responsabile di procedere alla designazione libera da indicazioni nominative e al Titolare di essere informato e di avere al limite un potere di opposizione.

Sui sub-responsabili devono essere imposti - anche in tal caso formalmente con un contratto o qualsiasi altro atto giuridico - gli stessi obblighi in materia di protezione dei dati che sono contenuti nel contratto fra Titolare e Responsabile del trattamento.

Non è prevista una "responsabilità solidale" fra i sub-responsabili e il responsabile del trattamento in quanto quest'ultimo mantiene, nei confronti del Titolare, l'intera responsabilità dell'adempimento degli obblighi (salvo eventualmente l'esercizio dell'azione di rivalsa nei confronti del sub-responsabile).

5.4 ——— La figura del DPO

Il Regolamento UE 2016/679, così come tutti ormai sappiamo, impone ai Titolari e Responsabili del trattamento l'onere di adottare tutti i comportamenti proattivi capaci di dimostrare di avere adottato concretamente le misure finalizzate ad assicurarne l'applicazione, il rispetto dei due essenziali criteri della "data protection by default" e "privacy by design" già al momento di configurare il trattamento dei dati personali predisponendo fin dall'inizio le garanzie indispensabili "a soddisfare i requisiti" del GDPR e tutelare i diritti degli interessati.

Tra le misure più rilevanti che sono prescritte dal legislatore comunitario senza dubbio c'è quella dell'obbligo, a carico di talune categorie di Titolari e Responsabili del trattamento, dell'introduzione della figura del Data Protection Officer, un nuovo professionista ad alta specializzazione che dovrà facilitare l'osservanza di tutti i principi del GDPR.

Si è parlato e si continua a parlare tantissimo di questa nuova figura, anche perché si tratta di un soggetto che, al momento, appare di difficile reperimento e sulla quale si è recentemente ripetutamente espressa anche l'Autorità Garante per la protezione dei dati personali e il Gruppo Articolo 29.

La figura del Data Protection Officer in realtà non costituisce una novità assoluta, almeno per molti paesi dell'Unione Europea.

Al riguardo va precisato che la Direttiva 95/46/Ce, che sarà abrogata tra pochi mesi, a maggio prossimo, quando diverranno applicabili le misure del RGDP, non prevedeva in realtà alcun obbligo di nomina di un professionista dedicato alle politiche della protezione dei dati personali, ma in molti Stati membri si è deciso che fosse obbligatoria la sua nomina, perché ritenuta importante, anzi essenziale per facilitare

l'osservanza della normativa e far maturare la cultura della protezione dei dati in ogni ambito aziendale.

Ad esempio una figura simile a quella del Data Protection Officer era già stata introdotta come obbligatoria in alcuni ordinamenti europei, tra cui la Repubblica Ceca, la Germania e l'Austria.

In altri ordinamenti la nomina di tale soggetto era al contrario facoltativa, come in Francia, dove a fronte della sua attivazione venivano alleggeriti gli oneri del Titolare del trattamento.

La versione in lingua italiana del Regolamento lo indica come "Responsabile della protezione dei dati", e tale terminologia potrebbe rendere facile associare tale figura a quella più nota del responsabile del trattamento, confondendone ruoli ed attribuzioni.

L'associazione di termini si ferma però solo al piano terminologico, perché le funzioni che il legislatore comunitario assegna ai due ruoli, quello del responsabile del trattamento e quello del Data Protection Officer sono ben diverse e assolutamente da tener distinte, come poi più tardi sarà evidente.

La differenza tra i due soggetti è di non poco conto, visto che il Data Protection Officer deve essere indipendente e autonomo, mentre il responsabile del trattamento dei dati deve agire seguendo solo e soltanto le istruzioni operative del Titolare del trattamento, un vincolo che impedisce al responsabile di godere dell'ampia indipendenza, tipica del ruolo del primo.

Per quanto riguarda il responsabile del trattamento dei dati personali il GDPR finalmente delinea con estremo dettaglio il ruolo dei soggetti ai quali vengono affidate attività che comportano un trattamento di dati personali al di fuori del contesto aziendale, cioè quelle figure che per prassi e convenzione venivano comunemente individuate e designate come "responsabili esterni del trattamento dei dati personali", la cui disciplina veniva, per così dire, mutuata sinora da quella dell'articolo 29 del decreto legislativo n.196 del 2003.

Ma tornando al tema del Data Protection Officer, questo quando e da chi deve essere nominato?

L'articolo 37 del Regolamento 679, che ha per oggetto "Designazione del responsabile della protezione dei dati" al riguardo prevede che il Titolare del trattamento e il Responsabile del trattamento debbano designare un responsabile della protezione dei dati se:

a) questa è una pubblica amministrazione ovvero;

b) le sue attività principali consistono in trattamenti che, per natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure

c) le sue attività principali consistono nel trattamento, su larga scala, di dati sensibili o giudiziari.

In sintesi l'obbligo di designazione del Data Protection Officer riguarda, per quanto di interesse di questo elaborato che affronta il tema della sua attivazione nel contesto sanitario:

a) le aziende sanitarie pubbliche Titolari o Responsabili del trattamento;

b) le aziende sanitarie private Titolari o Responsabili del trattamento, e le strutture che, anche con dimensioni limitate, effettuano attività di assistenza, cura o di analisi;

c) le aziende che, come Titolari o Responsabili, forniscono servizi o attività alle strutture sanitarie, se per questo trattano sistematicamente dati sensibili, genetici, giudiziari, biometrici o effettuano trattamenti che per la loro natura, il loro oggetto o, ancora, per le loro finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala.

Tra parentesi, il Regolamento 679 prevede che qualora i Titolari e Responsabili ritengano di non dover nominare un Data Protection Officer questi debbano opportunamente documentare le valutazioni compiute per stabilire se non è obbligatoria la sua nomina, in modo da poter dimostrare nel corso di qualsiasi controllo che l'analisi ha preso in esame correttamente tutti i fattori necessari ad adottare tale decisione.

La suindicata documentazione, che costituisce parte della documentazione necessaria a dimostrare la corretta gestione dei processi di trattamento dei dati personali e che può essere oggetto di richiesta dall'Autorità Garante Privacy, deve essere aggiornata qualora necessario, per esempio se i titolari o i responsabili intraprendono nuove attività o forniscono nuovi servizi che potrebbero rendere necessaria la nomina del DPO, suggerita comunque dal legislatore comunitario su base volontaria, come azione positiva di compliance.

Così come indicato nelle specifiche Linee Guida della primavera scorsa il Data Protection Officer non va in alcun caso confuso con referenti o strutture interne al contesto aziendale che si occupano correntemente di procedure e adempimenti legati alla protezione dei dati, così come con i consulenti variamente denominati che supportano il Titolare o il Responsabile del trattamento

Cioè i Titolari e i Responsabili del trattamento, compresi quelli che devono obbligatoriamente designare il DPO, possono legittimamente avvalersi di personale o consulenti esterni incaricati di incombenze relative alla protezione dei dati personali, ma in tal caso non devono esserci ambiguità in termini di denominazione, status e compiti di queste figure.

Così come indicato dal Gruppo articolo 29 è dunque assolutamente essenziale che in tutte le comunicazioni interne all'azienda e anche in quelle esterne, gli interessati o con l'Autorità Garante Privacy questi soggetti non siano in alcun modo indicati con la denominazione di Data Protection Officer.

A questo punto è opportuno soffermarsi sull'analisi che è obbligato a designare il Data Protection Officer sia il Titolare che il Responsabile del trattamento dei dati personali, che lo devono tempestivamente e adeguatamente coinvolgere in tutte le questioni riguardanti la protezione dei dati personali.

Questi lo deve designare nel caso in cui, delegato a effettuare attività di trattamento dei dati personali, si trovi nelle condizioni dei suindicati punti a,b,c.

A tale riguardo il Data Protection Officer designato da un Responsabile del trattamento si troverà a vigilare non solo sulle attività di trattamento dei dati effettuate per conto e su mandato di un Titolare del trattamento, ma anche sulle attività di trattamento dei dati personali effettuate da questi quando opera in qualità di autonomo Titolare del trattamento - per esempio, per quanto riguarda il trattamento dei dati concernenti il personale, le risorse informatiche, la logistica.

Quindi si prefigura una situazione in cui, all'interno almeno del contesto sanitario, a seconda di chi soddisfi i criteri relativi all'obbligatorietà della nomina, potrà essere il solo Titolare ovvero il solo responsabile, oppure sia l'uno sia l'altro a dover designare il Data Protection Officer.

Resta da capire a questo punto quali debbano essere i limiti e le caratteristiche della doverosa collaborazione che si dovrà instaurare tra il Data Protection Officer del Titolare e quello del Responsabile del trattamento dei dati personali e come questo rapporto vada a essere rappresentato nei contratti che dovranno disciplinare le responsabilità del trattamento affidate dal primo soggetto al secondo.

Di tale articolata questione pare non trovarsi alcuna traccia nel testo del Regolamento 679 e neppure nel relativo e corrispondente Considerando 97.

Il Data Protection Officer è un ruolo con particolare rilevanza esterna al sistema aziendale.

Infatti la sua designazione ed i relativi dati di contatto devono essere comunicati sia all'Autorità Garante Privacy che agli interessati ed ai collaboratori de Titolare o del Responsabile che lo ha nominato.

I dati di contatto del Data Protection Officer 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.

In questo senso, il poter raggiungere agevolmente il Data Protection Officer, pare assolutamente opportuno e raccomandabile che questi sia localizzato fisicamente nel territorio comunitario e che le sue comunicazioni siano effettuate nella lingua correntemente utilizzata dall'Autorità Garante Privacy.

La "trasparenza" del Data Protection Officer nei confronti degli interessati e dei collaboratori, come già detto è da intendersi come possibilità, da garantire anche attraverso un indirizzo mail o un recapito telefonico, di avere un solo e certo interlocutore di questi relativamente a tutte le istanze inerenti il trattamento dei dati personali.

Il Data Protection Officer diventa quindi, almeno per il sistema sanitario, un Ufficio Relazioni con il Pubblico dedicato limitatamente alle problematiche legate alla protezione dei dati personali ed all'esercizio dei diritti degli interessati.

Proprio per questo i suoi dati di contatto dovranno essere inseriti in ogni nota informativa sul trattamento dei dati prevista curiosamente sia dal decreto legislativo n. 196 del 2003 che dal regolamento 679 allo stesso articolo, il 13 e indicati per ogni attività di trattamento di dati nel registro di cui all'articolo 30 dello stesso regolamento.
Mentre per quanto riguarda tutti i collaboratori autorizzati dal Titolare o dal Responsabile del trattamento a trattare i dati personali il Data Protection Officer, come più di seguito dettagliato avrà il compito di informare e fornire consulenza sugli obblighi e sulle misure indicate dal regolamento 679.

Ma non basta, il Data Protection Officer diventa il punto di contatto tra il Titolare o il Responsabile che lo ha designato e l'Autorità Garante Privacy, con la quale deve cooperare per tutte le questioni connesse al trattamento dei dati personali,, consultandolo anche preventivamente quando necessario.

Il Data Protection Officer, comunque tenuto al rispetto delle norme in materia di segreto o riservatezza, deve in ogni modo facilitare l'accesso, da parte dell'Autorità Garante, ai documenti e alle informazioni necessarie per l'adempimento dei suoi compiti istituzionali, compresi quelli finalizzati all'esercizio dei poteri di indagine, correttivi, autorizzativi e consultivi.

Il suindicato onere di rispetto del segreto vuole assicurare che il Data Protection Officer possa essere direttamente e facilmente contattato sia dai collaboratori del Titolare o Responsabile che dagli interessati, assicurando la confidenzialità delle comunicazioni ricevute allo scopo di tutelare, in particolar modo, il rispetto dei diritti del lavoratore che vi si possa rivolgere.

Ma quali sono, oltrea quelli già indicati, i compiti di questo particolare professionista?

Il Regolamento 679 a questo riguardo indica come compiti del Data Protection Officer quelli di:
a) sorvegliare l'osservanza del regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del Titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, tra le quali sono da ricomprendere l'attribuzione delle diverse responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
b) fornire, qualora venga richiesto, un parere relativamente alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
c) controllare che le violazioni dei dati personali siano documentate, notificate e comunicate.

Il Data Protection Officer deve svolgere le sue funzioni valutando debitamente i rischi inerenti ai diversi trattamenti di dati personali, tenendo conto della loro natura, contesto, ambito di applicazione e finalità, definendo un ordine di priorità nell'attività svolta e concentrandosi sulle questioni che paiono presentare maggiori rischi in termini di protezione dei dati.

Per poter svolgere i compiti assegnatigli dal Regolamento 679 il Data Protection Officer può legittimamente accedere a tutte le informazioni necessarie ad individuare i trattamenti svolti per conto del Titolare o del Responsabile al fine di effettuare un analisi e verifica dei trattamenti in termini di loro conformità e eventuale necessità di rettifica.

Per quanto invece riguarda la valutazione di impatto sulla protezione dei dati, il Titolare o il responsabile sono tenuti a consultarsi con il proprio Data Protection Officer per decidere se questa ed in che modo debba essere effettuata e come eventualmente debba essere rimodulato il trattamento oggetto di valutazione.

Il Titolare o il Responsabile del trattamento devono fornire al Data Protection Officer le risorse necessarie per

assolvere ai compiti assegnati, comprese quelle necessarie a aggiornare e mantenere la propria conoscenza specialistica, dandogli supporto attivo da parte del senior management e un tempo sufficiente per l'espletamento dei compiti succitati.

Assicurare le risorse necessarie significa anche fornire al Data Prtoection Officer un supporto adeguato in termini di risorse finanziarie, infrastrutture (sede, attrezzature, strumentazione) e, ove opportuno, personale.

A tale proposito, in considerazione delle dimensioni e della struttura della singola azienda può essere necessario costituire un ufficio o un gruppo di lavoro che collabora con il Data Protection Officer, definendone dettagliatamente la struttura interna, i compiti e le responsabilità individuali.

Tali considerazioni appaiono del tutto ovvie nel caso di strutture aziendali complesse o articolate, perché quanto più aumentano complessità e/o sensibilità dei trattamenti, tanto maggiori devono essere le risorse messe a disposizione del Data Protection Officer, che deve poter operare con efficienza e contare su risorse sufficienti in proporzione al trattamento svolto.

Per poter svolgere senza alcuna pressione e ingerenza le sue delicate funzioni al Data Protection Officer sono assicurate dal regolamento 679 alcune garanzie essenziali per consentire di operare con un grado sufficiente di autonomia all'interno dell'organizzazione del Titolare o Responsabile, che devono assicurargli di non ricevere nessuna istruzione su come procedere con le proprie attività e di agire in maniera del tutto indipendente.

Da questo si deduce che il Data Protection Officer riferisce direttamente al vertice gerarchico del Titolare o Responsabile del trattamento dei dati personali o a chi lo rappresenta, nel caso delle aziende sanitarie, ad esempio, al direttore generale e che solo questi mantengono la piena responsabilità dell'osservanza della normativa in materia di protezione dei dati e devono essere in grado di dimostrarla.

Né, d'altra parte, il Titolare o il Responsabile del trattamento possono rimuovere il Data Protection Officer, che può essere reclutato tra i dipendenti o arruolato con uno specifico contratto di servizio, per l'adempimento dei suoi specifici compiti, l'esecuzione dei quali non può dare adito ad un possibile eventuale conflitto di interessi.

Nel merito il Titolare o il Responsabile del trattamento dei dati personali devono assicurarsi che il Data Protection Officer non svolga contemporaneamente altri compiti che possano generare tale conflitto, che potrebbe sorgere quando questi assuma contemporaneamente in azienda un altro ruolo che comporti la definizione delle finalità o modalità del trattamento di dati personali, come ad esempio riguardo a ruoli manageriali di vertice o posizioni gerarchicamente inferiori qualora queste comportino la determinazione di finalità o mezzi del trattamento.
Ma le particolarità che riguardano il ruolo del Data Protection Officer riguardano sia le caratteristiche, quelle di un professionista dotato anche di qualità manageriali ed organizzative, onde poter suggerire al Titolare o responsabile dei dati i più opportuni cambiamenti di carattere tecnico-organizzativo, che le competenze e le modalità di arruolamento.

Per quanto riguarda le competenze che deve possedere il Data Protection Officer questi può essere designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa sulla protezione dei dati personali e delle prassie procedure in materia di protezione dei dati, e della capacità di assolvere i suoi compiti.

Le Linee Guida succitate al riguardano indicano che il livello necessario di conoscenza specialistica dovrebbe essere determinato in base ai trattamenti di dati effettuati e alla protezione richiesta per i dati personali oggetto di trattamento su mandato del Titolare o Responsabile del trattamento dei dati personali.

Relativamente invece alle conoscenze specialistiche, questo deve essere proporzionato alla sensibilità, complessità e quantità dei dati sottoposti a trattamento; nel caso, ad esempio, di un trattamento che riveste particolare complessità oppure comporta un volume consistente di dati sensibili, il Data Protection Officer dovrà dimostrare di avere un livello più elevato di conoscenze specialistiche e di supporto, di conoscere le operazioni di trattamento svolte e lo specifico settore di attività e dell'organizzazione del Titolare o del Responsabile.

Per finire l'elenco dei requisiti richiesti al Data Protection Officer, questo deve possedere un'approfondita esperienza di coordinamento delle misure di protezione dei dati personali e, se intende operare in una pubblica amministrazione, come ad esempio in un'azienda sanitaria, deve avere anche una conoscenza approfondita delle norme e procedure amministrative applicabili.

Da tutto questo quadro emerge con chiarezza che quello di cui si sta trattando è una figura manageriale, indipendente, competente e in diretta relazione con i vertici aziendali, considerazione che renderebbe ovvia una particolare attenzione nello scegliere il proprio Data Protection Officer, una figura professionale nuova sul mercato, che necessita di una preparazione specialistica e una formazione continua ma anche di un'esperienza concreta sul campo per supportare adeguatamente le organizzazioni.

Quindi la selezione di questa nuova figura per l'azienda assume una importanza strategica. Come e dove reperirla? Il suo profilo ideale pare rispondere a quello di un professionista esterno all'azienda, dotato delle necessarie competenze, che svolge un ruolo "**scomodo**", in quanto potrebbe **entrare in conflitto con le effettive esigenze operative aziendali, nel quale il regolamento 679 riconosce** uno degli elementi-chiave all'interno del nuovo sistema di governance e protezione dei dati personali.

Insomma il Data Protection Officer rappresenta una figura chiave e protagonista nell'ambito del trattamento dei dati personali, figura che nel sistema sanitario è già da tempo individuata nelle Linee Guida e i Decreti sul Dossier e Fascicolo Sanitario Elettronico.
Ma l'indubbia apertura di uno spazio professionale in un contesto lavorativo come quello odierno hanno favorito l'attivazione di percorsi di formazione e sistemi di certificazione che, potendo indurre i Titolari o i Responsabili che devono, soprattutto nei contesti più critici di trattamento dei dati personali, come ad esempio quello sanitario, a operare scelte poco consapevoli dei propri Data Protection Officer, ha spinto l'Autorità Garante sia a Luglio che lo scorso 15 settembre, a chiarire con un proprio comunicato, come scegliere questo professionista.

Il pericolo altrimenti sarebbe quello che i Titolari o Responsabili possano affidarsi a professionalità prive dei necessari requisiti, con il rischio di subire le conseguenze di un'organizzazione e protezione inidonea dei trattamenti dei dati e vanificare le garanzie, di sicurezza prima di tutto, cui sono tenuti, nel cui caso potrebbero rispondere anche per l'ipotesi di *culpa in eligendo*.

Il comunicato citato, che ha per oggetto "Regolamento privacy, come scegliere il responsabile della protezione dei dati -Le prime indicazioni del Garante: necessarie competenze specifiche non attestati formali" chiarisce, proprio in risposta ai quesiti posti all'Autorità da un azienda sanitaria, che "le aziende sanitarie dovranno scegliere il Data Protection Officer con particolare attenzione, verificando la presenza di competenze ed esperienze specifiche, per le quali non sono richieste attestazioni formali sul possesso delle conoscenze o l'iscrizione ad appositi albi professionali"
Secondo l'Autorità, infatti "*..i Data Protection Officer delle aziende sanitarie dovranno avere un'approfondita conoscenza della normativa e delle prassi in materia di privacy, nonché delle norme e delle procedure amministrative che caratterizzano tale tipo di azienda e nella loro selezione sarà opportuno privilegiare chi può dimostrare qualità professionali adeguate alla complessità del compito da svolgere, magari documentando le esperienze fatte, ….e.. in considerazione della delicatezza dei trattamenti di dati effettuati (come quelli sulla salute o quelli genetici) dovranno preferibilmente vantare una specifica esperienza al riguardo e assicurare un impegno pressoché esclusivo nella gestione di tali compiti*".

L'Autorità ha inoltre chiarito che "la normativa attuale non prevede l'obbligo per i candidati di possedere attestati formali delle competenze professionali, che possono rappresentare un utile strumento per valutare il possesso di un livello adeguato di conoscenza della disciplina ma, tuttavia, non equivalgono a una "abilitazione" allo svolgimento del ruolo del DPO (o anche RPD, vedi sotto). La normativa attuale, tra l'altro, non prevede l'istituzione di un albo dei "Responsabili della protezione dei dati" che possa attestare i requisiti e le caratteristiche di conoscenza, abilità e competenza di chi vi è iscritto".

In conclusione, per l'Autorità Garante Privacy le aziende sanitarie nel selezionare il proprio Data Protection Officer dovranno valutare ".. autonomamente il possesso dei requisiti necessari per svolgere i compiti assegnati."

5.5 —— Informative e consensi

5.5.1 —— L'informativa

Con l'entrata in vigore del GDPR, l'informativa per il trattamento dei dati personali e sensibili dovrà essere ampliata rispetto a quella prevista dal Codice.
Principi generali

Resta invariato l'obbligo di fornire l'informativa prima della raccolta dei dati, se raccolti direttamente presso l'interessato, specificando l'identità del Titolare del trattamento, la finalità, i destinatari dei dati, i diritti degli interessati; se i dati non sono raccolti direttamente presso l'interessato vanno indicate anche le categorie dei dati oggetto del trattamento.

Il GDPR pone grande rilevanza su alcune caratteristiche indispensabili dell'informativa quali la chiarezza, la trasparenza e la facilità di comprensione da parte dell'interessato, ottenute anche attraverso l'utilizzo di icone - da abbinare comunque sempre al testo esteso - che dovranno essere identiche in tutta la UE e che verranno definite prossimamente dalla Commissione Europea;per i minori fino a 16 anni va prevista un'informativa con un linguaggio ancor più semplice e chiaro adatto alla loro comprensione.

L'informativa va data preferibilmente per iscritto e in formato elettronico, anche se è ammesso il formato orale.

I contenuti - art. 13

Le strutture sanitarie in sintesi devono fornire all'interessato le seguenti informazioni minime:

- L'identità e i dati di contatto del Titolare del trattamento
- I dati di contatto del Data Protection Officer (DPO)
- Le finalità del trattamento
- I destinatari o le categorie di destinatari dei dati personali
- L'intenzione del Titolare di trasferire i dati raccolti a un paese terzo
- Il periodo di conservazione dei dati personali raccolti
- I diritti dell'interessato relativamente ai propri dati (accesso, rettifica, cancellazione, portabilità, limitazione del trattamento)
- Il diritto per l'interessato di presentare reclamo all'autorità di controllo
- Le conseguenze del mancato conferimento dei dati personali
- L'esistenza di un processo di profilazione, la logica del processo e le conseguenze del trattamento per l'interessato.

L'informativa deve elencare quali trattamenti di dati vengono effettuati nella struttura e specificare per quali di essi è necessario il consenso dell'interessato o del tutore nei casi previsti (ad esempio non è necessario per il trattamento dei dati ai fini amministrativi o richiesto dalle istituzioni).
Le strutture sanitarie trattano infatti svariate tipologie di dati personali e sensibili, e in molti casi anche dati definiti "super-sensibili" come quelli sulla sieropositività, sulla dipendenza da alcool o droghe, su violenze subite ecc.; e ancora, dati genetici, dati relativi alla donazione di organi, per fini di ricerca, per campagne di prevenzione, marketing, comunicazione a case farmaceutiche, dati biometrici in caso di raccolta firma grafometrica ecc.
Si ricorda che le Strutture devono tenere e mantenere aggiornato un registro delle attività di trattamento effettuate al proprio interno.
Cosa cambia con il GDPR

- Esaminando l'elenco dei contenuti minimi dell'informativa secondo il GDPR, si evidenziano le seguenti novità rispetto al Codice:
- L'obbligo di indicare chiaramente i dati di contatto del DPO (detto anche RDP in Italia)
- Nel caso sia previsto il trasferimento di dati in Paesi terzi, va specificato attraverso quali strumenti e con quali garanzie

- Va indicato il periodo di conservazione dei dati raccolti
- Va specificato il diritto alla portabilità dei dati
- Va specificato il diritto di presentare un reclamo all'autorità di controllo
- Va dichiarato se il trattamento prevede un processo di profilazione degli interessati
- La struttura sanitaria dovrà riformulare il testo dell'informativa precedentemente predisposta secondo quanto richiesto dal Codice, aggiungendo le nuove informazioni richieste dal GDPR.

5.5.2 —— Un esempio di informativa per il trattamento dei dati personali e sensibili secondo il GDPR

Nella presente informativa sono riportate le informazioni relative al trattamento dei dati personali e sensibili effettuate da questa Struttura Sanitaria, secondo il vigente Regolamento dell'Unione Europea n.2016/679.
"Titolare del trattamento è XXX (inserire dati completi), a cui l'interessato potrà rivolgersi per far valere i Suoi diritti tramite l'ufficio URP sito in (indirizzo e telefono) o direttamente all'indirizzo email xxx@nomeospedale.it.
Il Responsabile della Protezione dei dati personali (DPO) è il sig.YYY, contattabile al numero di telefono nnnnnnnnn e all'indirizzo email yyy@nomeospedale.it.
L'elenco dei Responsabili dei trattamenti è presente sul sito web dell'Azienda www.ospedale.it e presso l'URP.

Trattamento dei dati personali e sensibili

Finalità - I dati personali e sensibili degli utenti verranno trattati per finalità di cura, solo previo consenso dell'interessato, amministrative e, esclusivamente previo consenso dell'interessato e nel rispetto del quadro normativo vigente, per finalità di ricerca scientifica, resi anonimi ovvero privati dei dati identificativi che possano ricondurre direttamente all'interessato.
Modalità del trattamento - I dati potranno essere trattati in forma cartacea ed elettronica, con accesso consentito ai soli operatori autorizzati, precedentemente nominati Responsabili o Incaricati del trattamento, i quali hanno seguito dei corsi di formazione specifici e vengono periodicamente aggiornati sulle regole della privacy e sensibilizzati al rispetto e alla tutela della dignità e della riservatezza del paziente.
Tutti gli operatori che accedono ai dati informatizzati sono identificabili e dotati di password personale; l'accesso ai dati è consentito solo per le finalità legate al ruolo dell'operatore e solo per lo stretto tempo necessario a trattare la prestazione per la quale il paziente si è recato presso la Struttura.
Tempo di conservazione dei dati - I dati personali e sensibili da Lei forniti e/o prodotti dalla nostra Struttura verranno conservati per il tempo previsto dall'attuale normativa : in particolare, i dati relativi a ciascun episodio di ricovero, raccolti nella relativa cartella clinica, verranno conservati a tempo indeterminato; i dati dei referti di laboratorio e di diagnostica verranno invece conservati per un anno e al termine di tale periodo verranno automaticamente cancellati dai nostri archivi elettronici, a meno che Lei abbia dato il consenso al loro inserimento nel Dossier Sanitario Elettronico o nel Fascicolo Sanitario Elettronico.
L'elenco dei trattamenti dei dati che la nostra Struttura può effettuare per l'assistito e il periodo di conservazione di ciascuna tipologia di dati è consultabile sul nostro sito web e presso l'URP.
Ambito di comunicazione e diffusione - I dati personali e sensibili non verranno in alcun modo diffusi, ma potranno essere trasmessi agli enti competenti per finalità amministrative o istituzionali, secondo quanto richiesto dalla normativa vigente.

Conseguenze del mancato consenso al trattamento - Il consenso al trattamento dei dati personali e sensibili è indispensabile per accedere alle cure richieste, senza di esso il paziente non potrà essere curato nella nostra Struttura. Il trattamento per fini amministrativi verrà effettuato nel rispetto del Regolamento per il trattamento dei dati sensibili e giudiziari adottato dalla Regione, sul quale l'Autorità Garante ha espresso parere favorevole.

Il consenso al trattamento per fini scientifici e di ricerca è facoltativo e il mancato consenso non preclude in alcun modo l'accesso alle prestazioni richieste.

L'interessato ha diritto in qualsiasi momento di modificare o revocare il consenso dato per ciascuno dei trattamenti, rivolgendosi all'URP.

Diritti dell'interessato - L'interessato può richiedere in qualsiasi momento l'elenco degli accessi effettuati ai propri dati, nonché la loro rettifica e la loro cancellazione ove quest'ultima non contrasti con la normativa vigente sulla conservazione dei dati stessi e con la necessità di tutelare in caso di contenzioso giudiziario i professionisti sanitari che li hanno trattati.; ha il diritto di richiedere la trasmissione dei propri dati a un altro operatore sanitario in un formato leggibile con le più comuni applicazioni ; ha il diritto di presentare reclamo all'autorità di controllo in caso di illecito trattamento o di ritardo nella risposta del Titolare a una richiesta che rientri nei diritti dell'interessato.

5.5.3 ——— Trattamento dei dati personali e sensibili tramite Dossier Sanitario

Il Dossier Sanitario Elettronico è uno strumento informatico che permette di raccogliere i dati relativi alle prestazioni effettuate da un paziente nella Struttura Sanitaria, e comprende referti, cartelle cliniche e altri documenti clinici prodotti in occasione dell'episodio di cura.

La consultazione del Dossier da parte dei professionisti sanitari consente di avere un quadro clinico del paziente più chiaro e permette ai professionisti stessi di formulare diagnosi più precise e di mettere in atto cure più appropriate.

La costituzione del Dossier Sanitario è comunque facoltativa e può avere luogo solo con il consenso dell'interessato, che può inoltre dare o meno il consenso all'inserimento nel Dossier anche dei dati relativi agli accessi precedentemente effettuati nella stessa Struttura e non ancora inseriti nel Dossier.

L'interessato può revocare in qualsiasi momento il consenso all'inserimento dei dati nel Dossier e alla consultazione dei dati precedentemente inseriti (oscuramento).

Il mancato consenso all'utilizzo dei dati personali e sensibili tramite Dossier non preclude l'accesso alle prestazioni e alle cure relative; in caso di diniego, tali dati resteranno a disposizione del professionista sanitario che ha generato tali dati e, per la sola durata di esecuzione della prestazione, del personale sanitario autorizzato afferente al reparto che ha in cura il paziente.

5.5.4 ——— Trattamento dei dati personali e sensibili tramite Fascicolo Sanitario Elettronico

Il Fascicolo Sanitario Elettronico, governato dalla Regione (o dalla Provincia Autonoma), è l'insieme di dati e documenti digitali di tipo sanitario e socio-sanitario, relativi a eventi clinici presenti e trascorsi che riguardano l'assistito, generati da strutture sanitarie, socio-sanitarie e dai medici di base.

La consultazione del Fascicolo Sanitario Elettronico da parte dei professionisti sanitari consente di avere un

quadro unclinico più chiaro del paziente e permette ai professionisti stessi di formulare diagnosi più precise e di mettere in atto cure più appropriate.
Il FSE verrà alimentato con i dati che riguardano l'interessato raccolti e/o prodotti nella nostra Struttura solo previo consenso dell'interessato, che potrà esercitare in qualsiasi momento il diritto di revoca del trattamento.
L'interessato dovrà esprimere un consenso per l'alimentazione del FSE e un consenso separato per la consultazione del FSE, richiesto per rendere il Fascicolo accessibile agli operatori sanitari che prenderanno in cura l'interessato.
Il mancato consenso all'alimentazione del FSE con i propri dati personali e sensibili e/o alla sua consultazione non preclude l'accesso alle prestazioni e alle cure relative nella nostra Struttura; in caso di diniego all'alimentazione, tali dati non verranno inseriti nel FSE e resteranno nella nostra Struttura a disposizione del personale sanitario autorizzato afferente al reparto/servizio che sta curando il paziente, per la sola durata di esecuzione della prestazione a meno che sia stato dato il consenso per il loro inserimento nel Dossier Sanitario; in caso di diniego alla consultazione tramite FSE, o in caso di richiesta di oscuramento dei dati ivi contenuti successivamente al loro inserimento nel FSE, i dati e i documenti contenuti nel FSE potranno essere consultati esclusivamente dall'interessato e dai titolari che hanno generato i predetti documenti.

5.5.5 ——— Gestione del consenso

La gestione in modalità nativa digitale dei consensi, che richiede quindi la firma dell'interessato, rappresenta ad oggi "l'ultimo miglio" nel percorso verso la gestione completamente digitale dai dati sanitari dei pazienti, garantendo pieno valore legale della documentazione e dei processi di supporto. Su questo tema esistono tecnologie, normative e standard di supporto consolidati. Mancano però ancora linee guida specifiche, regionali o nazionali, che indirizzino una struttura sanitaria che voglia completare "l'ultimo miglio" verso uno scenario completamente digitale.
Una struttura sanitaria che voglia intraprendere un progetto di gestione digitale dei consensi deve porre l'attenzione e presidiare puntualmente, in termini di competenze sul campo, diversi fronti: aspetti tecnologici (come fare), organizzativi (revisione dei processi) e normativi nel rispetto della legislazione vigente in ambito sanitario, di dematerializzazione e della privacy.
La dematerializzazione dei consensi in ambito clinico è quindi ancora un percorso complesso la cui attuazione abiliterebbe significativi benefici, garantendo la gestione di informazioni strutturate che consentirebbero di limitare l'archiviazione, la conservazione e l'accesso al dossier del paziente o a specifici documenti clinici elettronici (DCE) alle sole persone che dispongono dei diritti operativi e di visibilità specificatamente richiesti.
È importante distinguere tra le diverse categorie di consenso, perché l'approccio tecnologico e organizzativo in questi tre macro scenari può essere significativamente differente.
A questo scopo, possiamo suddividere i consensi in tre macro categorie:

- il consenso al trattamento dati (riferimento normativa sulla privacy 196/2003);
- il consenso al dossier e/o al fascicolo sanitario elettronico;
- il consenso informato (differente caso per caso e relativo alla specifica prestazione sanitaria da erogare).

Tra i consensi si annoverano poi anche quelli relativi a specifici trial clinici e di ricerca, all'invio di messaggistica personalizzata, all'adesione a campagne di prevenzione, ad un piano assistenziale integrato (PAI o PDTA), all'uso della firma elettronica avanzata (FEA) ed altri ancora.

Per esemplificare le differenze, anche in termini di impatto e gestione dal punto di vista tecnologico, consideriamo due diverse tipologie di consenso: il consenso al trattamento dati comunemente definito come "consenso privacy", e il consenso informato. Nel primo caso:
in Sanità può essere registrato oralmente purché venga prodotto un documento informatico che ne attesti la raccolta da parte di un operatore qualificato della struttura sanitaria che a sua volta sottoscrive il documento di raccolta apponendo la propria firma digitale;
l'informativa ad esso associata, se opportunamente divulgata in modalità quanto più possibile multicanale verso il paziente (sito internet, posta elettronica, cartellonistica, …) può essere letta in autonomia dall'interessato e non necessita obbligatoriamente né di un medico né di un operatore sanitario che provveda in modalità preventiva alla sua illustrazione o spiegazione;
può essere rilasciato una tantum e valere fino a revoca esplicita del paziente;
abilita l'accesso ai dati sanitari dell'interessato nei diversi sistemi informativi della struttura sanitaria che lo ha in cura.

Nel caso del consenso informato, invece, vincolante rispetto alla erogazione di una specifica prestazione sanitaria quale un intervento chirurgico, un protocollo di chemioterapia, una trasfusione o qualsiasi altra metodica o trattamento per la quale è opportuno una puntuale informazione del paziente e, quindi, una sua esplicita assunzione di responsabilità, non è possibile la raccolta orale anche se effettuata da parte di un operatore qualificato.
In questo caso ci si ritrova in uno scenario in cui:

- il consenso deve essere raccolto per ogni singola prestazione (anche se della stessa tipologia);
- l'informativa deve essere illustrata e spiegata al paziente da un medico;
- il consenso non è revocabile dopo aver effettuato la prestazione;
- il consenso è vincolante rispetto alla possibilità di espletare la prestazione;
- il paziente deve poter sottoscrivere in maniera da garantire la piena validità legale per accettazione e conferma del consenso nonché presa visione e ricezione della relativa informativa.

Si deve poi considerare anche il tema dell'oscuramento/autorizzazione, che ha le seguenti caratteristiche:

- è un'informazione che scatta obbligatoriamente per legge o per volontà espressa dell'interessato (si produce un documento informatico per garantirne la tracciabilità in un contesto"document oriented' dematerializzato);
- non ha alcuna informativa associata;
- è relativo ad uno o più DCE e ne influenza la visibilità da parte degli utenti dei sistemi informativi delle strutture sanitarie (dossier) e del FSE.

Nell'ambito del Technical Framework di IHE (Integrating Healthcare Enterprises) alcuni associano il concetto dell'oscuramento al confidentiality code, metadato previsto nell'Affinity Domain del profilo XDS (Cross Document Sharing). In realtà il confidentiality code è un dato che viene, nella maggior parte dei casi, assegnato dall'applicazione che produce il documento a fronte di considerazioni basate su normative, si tratta di una informazione la cui valorizzazione iniziale resta permanente poiché associata al contenuto del documento; può influenzare l'oscuramento pur non essendo l'unico elemento che può farlo, ma soprattutto l'oscuramento può variare nel tempo, le due informazioni sono pertanto da intendersi non correlate.

5.5.6 ——— Metodi di Acquisizione dei consensi digitali

L'acquisizione dei consensi digitali può avvenire con differenti metodi e soluzioni tecnologiche la cui individuazione e scelta, rispetto alla adattabilità ai propri processi, è lasciata alla discrezione della singola struttura sanitaria che avvia un percorso di dematerializzazione del consenso: non esistono al momento specifiche linee guida nazionali.

Si riportano sinteticamente i metodi più comuni ed utilizzabili nel contesto e normativo italiano per la raccolta della firma elettronica da parte del paziente sui documenti informatici di consenso non dimenticando di tenere presenti i disposti del regolamento europeo eIDAS 910/2014[23]e del nuovo CAD in fase di modifica:

- Firma elettronica semplice
- Firma Elettronica Avanzata grafometrica anche di tipo biometrico (FEA - GFM)
- Firma Elettronica Avanzata - Carta Nazionale dei Servizi (FEA-CNS)/OTP etc.
- Firma digitale qualificata
- Servizio Pubblico di Identità Digitale (SPID)

Il consenso digitale come strumento per ottemperare alle regole di archiviazione e di consultazione dei DCE e del dossier sanitario.

Una volta acquisiti, i consensi digitali influenzano tutti i flussi documentali aziendali.

I DCE infatti per poter essere archiviati, conservati e consultati in una logica di dossier, dovrebbero essere soggetti a controlli rispetto alle volontà espresse nei consensi stessi dai pazienti e a quanto dettato dalle normative vigenti.

In questo contesto, un progetto di reale ed efficace gestione digitale del consenso non può non prevedere, nell'ambito dell'architettura applicativa della struttura sanitaria, una specifica soluzione applicativa che gestisca tutte le problematiche legate all'applicazione delle policy di privacy in ottemperanza anche del regolamento europeo.

L'applicazione informatica dovrebbe permettere la definizione di regole, la verifica della liceità degli accessi alla documentazione contenuta nei repository aziendali e l'interoperabilità con tutte le risorse in grado di fornire informazioni utili per la corretta applicazione delle regole.

L'adozione di una soluzione applicativa non deve essere invasiva rispetto all'architettura del sistema informativo sanitario, deve infatti operare all'interno del flusso documentale XDS, senza cambiarne le caratteristiche, garantendo che sia il "Document Source" che il "Document Consumer" continuino a invocare le stesse tipologie di servizi e possano ottenere le stesse tipologie di risposte.

La soluzione applicativa di gestione del consenso dovrebbe quindi intercettare, con la componente PEP (Policy Enforcement Point), gli accessi alla documentazione e attraverso la sua componente PDP (Policy Decision Point) applicare le regole che sono state precedentemente impostate attraverso le interfacce della componente PAP (Policy Administration Point) a loro volta manutenute nel PRP (Policy Repository Point).

PEP Policy Enforcement Point	è la componente che intercetta la richiesta di trattamento di un documento, sia produzione che consultazione, ingaggia il PDP per applicare le regole
PDP Policy Decision Point	è la componente che, ingaggiata dal PEP, applica le regole descritte attraverso le policy associate a ogni specifico codice di consenso, incrociandole con il ruolo dell'utente che sta accedendo.
PAP Policy Admin Point	è l'insieme delle funzionalità attraverso le quali si gestiscono le policy associate a ogni codice di consenso, descritte utilizzando i formalismi XACML
PRP Policy Repository	è il repository dove vengono salvate le policy gestite dal PAP
PIP Policy Information Point	è la componente che detiene o recupera le informazioni necessarie alla corretta applicazione delle regole che descrivono le policy attraverso i formalismi XACML
PIPprobe	Si tratta della componente locale del PIP che ha il compito di interoperare con le fonti di informazioni necessarie per la corretta applicazioni delle regole. Può essere adattata alle specificità delle componenti locali presenti nel S.I. dell'Azienda.

23. http://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX%3A32014R0910&from=EN

Figira - Componenti applicative dei profili privacy - IHE

A livello funzionale, le soluzioni devono interoperare con il mondo esterno attraverso metodologie standard o ispirate a profili di interoperabilità IHE:

- XDS Cross Enterprise Document Sharing, che descrive i rapporti tra i produttori di documentazione, i consumatori, il repository e il registry;
- PLT Patient Location Tracking, il cui fine è quello di tracciare puntualmente la localizzazione del paziente grazie alle informazioni ricevute dagli applicativi che ne gestiscono le attività;
- SER Secure Retreive, che descrive come eseguire accessi controllati alla documentazione clinica.

In occasione degli annuali Connectathon (www.ihe.net) è stata verificata l'efficienza e la completezza delle transazioni che descrivono i flussi di interoperabilità tra le componenti applicative coinvolte.
Per completezza di informazione di seguito un elenco di alcune tra le principali con la descrizione del conteso di utilizzo:

ITI-41 È usata dal Document Source per inviare il documento corredato di metadati.
Chi produce i documenti (Document Source), invia il documento verso il Repository con questa transazione.

ITI-18 Serve al Document Consumer per interrogare il Registry e ricevere l'elenco dei documenti presenti nel Repository che corrispondono alla ricerca.
Chi vuole accedere alla documentazione utilizza una applicazione che svolge il ruolo di Document Consumer, utilizza la transazione [ITI-18] per interrogare il Registry XDS dal quale riceverà l'elenco della documentazione presente sul repository.

ITI-43 È utilizzata dal Document Consumer per accedere a uno specifico documento selezionato dall'elenco prodotto dalla ITI-18.
Sulla base della risposta del Registry a fronte di una [ITI-18], il Document Consumer perfeziona la sua richiesta di accesso a uno o più documenti con la transazione [ITI-43].

ITI-76 Patient Location Tracking Feed.
È originata da una applicazione, che opera come attore "Patient Location Tracking Supplier" per registrare e comunicare al Patient Location Tracker Manager:
- la presa in carico di un Assistito presso una U.O.
- il trasferimento da una U.O. a un'altra
- la dimissione da una U.O., cioè il termine della presa in carico presso l'U.O.

ITI-77 Patient Location Tracking Query.
È l'interrogazione verso il DB del Patient Location Manager, eseguita dall'applicazione che vuole conoscere l'attuale localizzazione dell'Assistito.

Quanto veicolato attraverso le transazioni descritte è regolamentato dalle definizioni contenute nel documento denominato"Affinity Domain', così come descritto nelle specifiche del profilo XDS di IHE, questo documento deve essere esteso per prevedere la presenza e le regole di congruenza dei metadati riferiti al consenso al trattamento dei dati.
La consultazione dei documenti che descrivono la presenza del consenso avviene attraverso interrogazioni mirate del Registry XDS attraverso la transazione [ITI-18].

Attraverso l'utilizzo della [ITI-18] può essere invece verificata la presenza dello specifico consenso al momento del suo utilizzo, ad esempio in una struttura sanitaria che è anche un centro di ricerca e sede universitaria si potrebbero definire i seguenti consensi specifici:

DocumentTypeCode	Note
Consenso all'uso della FEA	Consenso Aziendale raccolto UNA TANTUM (fino a revoca)
Consenso al trattamento dati	Consenso Aziendale raccolto UNA TANTUM (fino a revoca)
Consenso al dossier	Consenso Aziendale raccolto UNA TANTUM (fino a revoca)
Consenso al dossier storico	Consenso Aziendale raccolto UNA TANTUM (fino a revoca)
Consenso informato<x>	Consenso Aziendale raccolto per ogni prestazione
Consenso trattamento dati Ricerca e Didattica	Consenso Aziendale raccolto UNA TANTUM (fino a revoca)
Consenso Trial <x>	Consenso Aziendale raccolto per ogni clinical Trial (fino a revoca)

L'adozione delle indicazioni descritte nel Technical Framework IHE deve influenzare positivamente la progettazione delle soluzioni applicative coinvolte nell'intero processo di gestione dei DCE, le soluzioni si devono arricchire di controlli applicativi che rendono il processo più complesso ma più efficace e garantito rispetto all'accessibilità del dato clinico da parte dei professionisti sanitari abilitati.

Si riporta di seguito una schematizzazione ad alto livello esemplificativa di come la soluzione applicativa per la gestione centralizzata del consenso CoM (Consent Manager) potrebbe operare nell'ambito di una comune architettura applicativa di una struttura sanitaria. Nello specifico le regole possono essere definite utilizzando tutte le informazioni che CoM, attraverso la componente PIP, è in grado di reperire. Per permettere a PIP di interoperare con le risorse che devono fornire le informazioni previste, è quindi essenziale realizzare tutte le integrazioni con le diverse applicazioni cliniche che detengono i dati (ad es. cartella clinica elettronica CCE, applicazione di pronto soccorso ed altri). Questa componente applicativa diventa fondamentale abilitando anche la gestione puntuale dell'accesso al dossier del paziente da parte dei professionisti sanitari secondo il criterio del "paziente in cura", come peraltro richiesto dalle linee guida in materia di dossier sanitario (Garante - giugno 2015).

È importante ricordare come nella progettazione, debba essere tenuto conto del fattore non improbabile che un consenso possa essere revocato e prevedere quindi un processo di gestione della revoca stessa con tutti gli impatti afferenti.

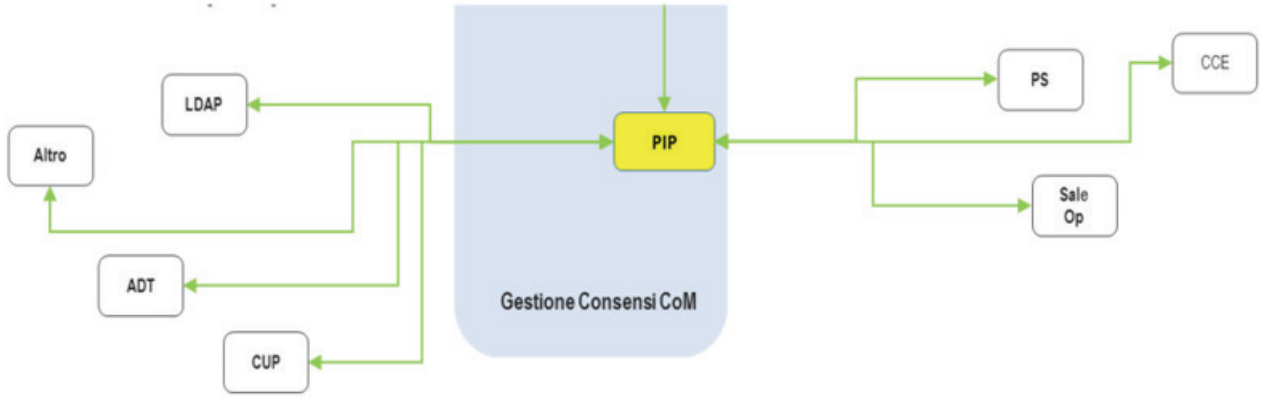


Figura: Esempio di architettura applicativa in un contesto di gestione digitale e centralizzata del consenso

5.6 —— I diritti dell'interessato

Si segnala che il rifreimento normativo del GDPR è al Capo III - I diritti dell'interessato. Su questo è previsto un regime sanzionatorio di cui all'art. 83 comma 5 lett a) che prevede sanzioni amministrative pecuniarie fino a 20 000 000 EUR, o per le imprese, fino al 4 % del fatturato mondiale totale annuo.

Il nuovo Regolamento centralizza ulteriormente il ruolo dell'interessato, che deve essere messo nelle condizioni di avere il controllo dei propri dati.
Il considerando 7 infatti così precisa:

- è opportuno che le persone fisiche abbiano il controllo dei dati personali che li riguardano e che la certezza giuridica e operativa sia rafforzata tanto per le persone fisiche quanto per gli operatori economici e le autorità pubbliche;
- da tale riconoscimento giuridico discendono molteplici diritti in capo agli interessati di cui il Titolare del trattamento deve essere a conoscenza;
- è infatti pacifico che nel momento in cui il Titolare decida di trattare i dati, le modalità di tale trattamento dovranno tener conto della possibile attivazione da parte dell'interessato dei propri diritti.

Le tipologie dei diritti degli interessanti

I diritti degli interessati possono essere suddivisi in due marcoaree: i diritti conoscitivi ed diritto di controllo.
In relazione ai diritti degli interessanti si è ritenuto - per facilitare la lettura - di inserire per ogni diritto gli articoli ed i Considerando di riferimento.

DIRITTI CONOSCITIVI

Diritto all'informativa **Art.13-14** Considerando 58, 60	Le persone interessate hanno il diritto di ricevere preciso informazioni sul trattamento dei dati. l'informativa deve contenere le seguenti informazioni: identità del titolare identità del data protection officer finalità del trattamento base giuridica eventuale legittimo interesse che costituisce la base giuridica eventuali obblighi di legge o di contratto in base ai quali i dati vanno forniti ambito di circolazione dei dati (UE o extra UE) durata del trattamento (eventuale) processo decisionale alla base del trattamento automatizzato diritti dell'interessato: accesso, rettifica, integrazione cancellazione, limitazione opposizione, portabilità, reclamo ad una autorità garante, revoca del consenso
Diritto all'accesso **art. 15** Considerando 63	L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in tal caso, di ottenere l'accesso ai dati personali

DIRITTI DI CONTROLLO

Diritto alla portabilità **Articolo 20** Considerando 68, 73	Si tratta dei un diritto nuovo L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti da un titolare del trattamento Ha altresì il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora: a) il trattamento si basi sul consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), o dell'articolo 9, paragrafo 2, lettera a), o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b); e b) il trattamento sia effettuato con mezzi automatizzati sul diritto alla portabilità è stato emanato un parere da parte del Gruppo di lavoro 29 WP 29
decisioni basate unicamente sul trattamento dei dati **Articolo 21 comma 2, 3** Considerando 70	L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona. Qualora i dati personali siano trattati per finalità di marketing diretto, l'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano effettuato per tali finalità, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto.

DIRITTI DI CONTROLLO

Diritto di rettifica e integrazione **Art. 5 (1) (d), 16** Considerando 39, 59, 65, 73	L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.
Diritto alla cancellazione e oblio **Art.17** Considerando 65-66, 68	L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste determinati motivi
Diritto alla limitazione **Articolo18** Considerando 67	L'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento quando ricorre determinate circostanze
Diritto all'opposizione **articolo 21** Considerando 50, 59, 69-70, 73	L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f), compresa la profilazione sulla base di tali disposizioni. Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria

Cooperazione con le Autorità (i "Garanti "degli Stati Membri) (art. 31)	I Titolari (ed i loro rappresentanti, se del caso) sono tenuti a collaborare, su richiesta, con le Autorità nello svolgimento dei loro compiti.
La sicurezza dei dati (art. 32)	Il Titolare deve attuare le misure di sicurezza tecniche e organizzative adeguate per proteggere i dati personali dalla distruzione accidentale o illecita, la perdita, la modifica, la rivelazione non autorizzata o l'accesso A seconda della natura del trattamento, tali misure possono comprendere (ad esempio): la cifratura dei dati personali; ridondanza e di back-up; test di sicurezza regolari. è importante ricordare che " L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo."
Data Breach (art. 33)	Nel caso di una violazione dei dati, il titolare deve comunicare formalmente tale violazione all'Autorità Garante, senza indebito ritardo, e in ogni caso entro 72 ore dalla conoscenza. Il titolare deve tenere un registro di tutte le violazioni dei dati, che comprende i fatti e gli effetti della violazione e qualsiasi azione per porvi rimedio. (art. 33) Il rispetto del termine di 72 ore per la segnalazione di violazioni dei dati al Garante rischia di rivelarsi estremamente impegnativo, in quanto richiederà alle aziende di individuare, esaminare e riferire le violazioni dei dati in un tempo molto ridotto. Tutte le violazioni dei dati devono essere inclusi nei documenti aziendali di gestione dei dati Tutte le violazioni devono essere registrate (anche quelle piccole e di scarso impatto), e questi record devono essere comunicati al Garante. Inoltre, gli obblighi di comunicazione ai sensi della direttiva e-privacy continuano a trovare applicazione per i fornitori di telecomunicazioni. Su questo punto in sede di emanazione del nuovo Regolamento e-privacy a si auspica in un raccordo dei due adempimenti.

5.6.1 ——— Modalità per l'esercizio dei diritti (art. 12)

Il Titolare del trattamento è tenuto a soddisfare le richieste dell'interessato circa l'esercizio dei suoi diritti. Deve quindi adottare tutte le misure che consentono di fornire all'interessato tutte le informazioni richieste in relazione al diritto attivato (es. l'interessato chiede l'opposizione al trattamento dei suoi dati oppure la portabilità).

Tali informazioni devono essere fornite "senza ingiustificato ritardo" e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa.

5.7 ——— Portabilità dei dati

Riferimenti Normativi

La portabilità dei dati è un nuovo requisito introdotto dall'art. 20 del GDPR:

1. *L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un Titolare del trattamento e ha il diritto di trasmettere tali dati a un altro Titolare del trattamento senza impedimenti da parte del Titolare del trattamento cui li ha forniti qualora:*
   a) il trattamento si basi sul consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), o dell'articolo 9, paragrafo 2, lettera a), o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b); e
   b) il trattamento sia effettuato con mezzi automatizzati.
2. *Nell'esercitare i propri diritti relativamente alla portabilità dei dati a norma del paragrafo 1, l'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un Titolare del trattamento all'altro, se tecnicamente fattibile.*
3. *L'esercizio del diritto di cui al paragrafo 1 del presente articolo lascia impregiudicato l'articolo 17. Tale diritto non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento.*
4. *Il diritto di cui al paragrafo 1 non deve ledere i diritti e le libertà altrui.*

È utile sottolineare che il diritto si applica ai dati personali **forniti al Titolare**, non a quelli generati da quest'ultimo.

Questo affermazione può sembrare che restringa il campo a poche categorie, a tal proposito risulta utile consultare il WP242, ovvero le Linee-guida sul diritto alla "portabilità dei dati"[24] dell'Art.29 Working party.

L'implementazione di questo requisito posto dal GDPR trae vantaggio:

dalla raccolta dei dati in un numero limitato di repository dai quali possano essere estratti con facilità in modo completo

dall'adozione diffusa di standard di settore diffusi, come l'HL7; il supporto di questi standard dovrebbero essere un requisito per ogni applicazione o middleware adottato, per il quale sia previsto il ruolo di repository primario di dati personali.

Per quanto riguarda **la portabilità** dei dati quindi, la Struttura Sanitaria deve dotarsi di applicativi che permettano di produrre, in un formato elettronico leggibile con i più comuni strumenti software, i referti e le cartelle

24. http://194.242.234.211/documents/10160/5184810/Linee-guida+sul+diritto+alla+portabilit%C3%A0+dei+dati+-+WP+242.pdf

cliniche archiviati nel Sistema. Questo requisito è ormai fondamentale anche in vista dell'implementazione del Fascicolo Sanitario Elettronico, che in alcune regioni d'Italia è già in funzione, nonché dell'integrazione con i Medici di Medicina Generale e con le Strutture Territoriali, che va prendendo sempre più piede.

5.8 —— Data protection agreement con terze parti

Accordo tra Titolare e Responsabile

Nei casi in cui un'attività di trattamento di dati personali viene svolta da un soggetto diverso rispetto al Titolare del trattamento è necessario definire la relazione fra il Titolare e il soggetto terzo, che potrebbe essere un altro Titolare (Cotitolarità) o un responsabile del trattamento. Vi è anche la possibilità che si instauri un rapporto tra responsabili del trattamento. Il capitolo che segue analizza esclusivamente il rapporto che si potrebbe creare tra un Titolare ed un Responsabile, toccando incidentalmente il rapporto tra Responsabili (Infra: p.XXX Ricorso ad altri Responsabili e Subresponsabili).

Il Titolare del trattamento definisce le finalità e i mezzi del trattamento, mentre il responsabile del trattamento deve trattare i dati secondo le istruzioni impartite dal Titolare, garantendo un corretto trattamento dei dati a cui accede al fine di offrire il servizio richiesto dal Titolare.

Di seguito sono elencati alcuni degli aspetti essenziali da definire nel documento di nomina a responsabile del trattamento, questo può assumere la forma di lettera di nomina, contratto o altro atto giuridico, in ogni caso un atto utilizzato per formalizzare e definire il rapporto tra Titolare e Responsabile con riguardo al trattamento di dati personali.

Alla lettera h comma 3 dell'articolo 28 del regolamento troviamo un principio generale di trasparenza dell'operato del Responsabile nei confronti del Titolare, infatti il primo deve rendere disponibili al secondo tutte le informazioni necessarie atte a dimostrare il rispetto del contratto o altro atto giuridico e deve essere disponibile a subire ispezioni da parte del Titolare o di un suo incaricato poiché questi ha l'onere di assicurarsi che il responsabile del trattamento nominato, offra sufficienti garanzie di conformità al Regolamento.

[Riferimento al DPA] Punto 2.3.2 del DPA - Rendicontazione, audit e collaborazione

Il Responsabile mette a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente atto, consente e contribuisce alle attività di revisione, comprese le ispezioni, realizzate dal Titolare o da un altro soggetto da questi incaricato.

Il Titolare del trattamento deve fornire istruzioni precise sulle modalità di trattamento dei dati ed elencare che tipo di dati sono trattati e per quali finalità. In particolare deve essere indicato se è prevista la comunicazione dei dati a terzi e se sono previsti trasferimenti transfrontalieri dei dati oggetto dell'accordo.

[Riferimento al DPA] Punto 2.5 del DPA - Comunicazione a terzi

Se il responsabile intende trasferire tutti o alcuni dati personali oggetto dell'Accordo verso un paese terzo o un'organizzazione Internazionale, si impegna ad informare il Titolare prima di procedere al trasferimento, fornendo indicazioni sulla base legale che legittima il trasferimento.

Il responsabile del trattamento può autonomamente assumere decisioni in ambito tecnico ed organizzativo con riguardo al servizio che sta offrendo; in nessun caso potrà variare le finalità e modalità del trattamento definite dal Titolare, né potrà usare i dati per propri scopi.

[Riferimento al DPA] Punto 2.2.2- Obblighi generali del Responsabile

Il Responsabile utilizza i dati personali oggetto del trattamento solo per le finalità indicate nell'Allegato A "Attività di trattamento", in nessun caso potrà utilizzare i dati per fini propri.
Le modalità tramite cui si perseguono le finalità devono anch'esse essere definite dal Titolare, il Responsabile si deve strettamente attenere alle sopracitate istruzioni. Nel caso il Responsabile decida di usare i dati per scopi propri ovvero per finalità o tramite mezzi non corrispondenti a quanto definito dal Titolare, sarà considerato a sua volta un Titolare per le attività di trattamento per le quali ha definito le finalità e/o i mezzi in autonomia.

Riferimenti Normativi

Art. 28 c.10 del Regolamento 2016/679 - Responsabile del trattamento

Fatti salvi gli articoli 82, 83 e 84, se un responsabile del trattamento viola il presente regolamento, determinando le finalità e i mezzi del trattamento, è considerato un Titolare del trattamento in questione.
Deve essere stabilita la forma tramite cui il responsabile del trattamento garantisce la confidenzialità dei dati con riferimento ai soggetti che li tratteranno. Il Regolamento richiede che il Responsabile garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate abbiano un adeguato obbligo legale alla riservatezza. Se l'obbligo legale può derivare dal segreto professionale l'impegno alla riservatezza potrebbe scaturire da un accordo di non divulgazione (NDA).
Deve essere definito in carico al responsabile del trattamento, l'obbligo di adozione di misure di sicurezza tecniche ed organizzative idonee a garantire la sicurezza dei dati. Le misure dovranno essere commisurate al rischio per diritti e libertà degli interessati e dovranno in ogni caso soddisfare i requisiti del regolamento.
[Riferimento al DPA] Punto 2.15- Obblighi generali del Responsabile
Tenendo conto della natura, dell'oggetto, del contesto e delle finalità del trattamento, ma anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il Responsabile del trattamento mette in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio.
In ogni caso il Responsabile sarà tenuto a garantire:
la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi in uso
la capacità di ripristinare la disponibilità e l'accesso ai dati in caso di incidente
la verifica e valutazione periodica dell'efficacia delle misure tecniche e organizzative
Questione che merita attenzione è la definizione della possibilità, e nel caso della modalità autorizzativa, affinché un responsabile possa nominare altri responsabili (Subresponsabili). Si prospettano almeno tre differenti modalità autorizzative:
Il responsabile non può ricorre o nominare ad altro responsabile, senza previa espressa e scritta autorizzazione del Titolare.
Il responsabile è autorizzato a nominare altro responsabile per lo svolgimento delle attività di trattamento.
Il responsabile è autorizzato a nominare altro responsabile previa notifica al Titolare salvo suo diritto di opposizione.

Fermo restando che agli eventuali Subresponsabili dovranno essere imposti gli stessi obblighi del primo responsabile e questi sono solidalmente responsabili in caso di risarcimento danno.
[Riferimento al DPA] Punto 2.7.1 Requisiti minimi da imporre ad altri Responsabili e Subresponsabili

Qualora il Responsabile nomini altro Responsabile del trattamento su tale altro responsabile del trattamento sono imposti mediante atto scritto, gli stessi obblighi in materia di protezione dei dati contenuti nel presente atto.

Per quanto riguarda l'esercizio dei diritti da parte degli interessati, i quali si possono alternativamente rivolgere a Titolare, Responsabile ed eventuali Subresponsabili, occorre stabilire se ed in che forma il responsabile del trattamento assista il Titolare nel caso un interessato intenda esercitare un diritto quale, quello di accesso ai dati, rettifica, oblio/cancellazione, limitazione del trattamento, portabilità dei dati, opposizione al trattamento, ecc..

Premettendo che l'obbligo di dare seguito alle richieste per l'esercizio di diritti degli interessati sta in capo al Titolare, questo può richiedere al Responsabile di assisterlo nel soddisfare le richieste degli interessati oppure delegare il Responsabile a dare seguito in autonomia alle richieste degli interessati.

[Riferimento al DPA] Punto 2.10 Diritti dell'interessato

Il Responsabile assiste il Titolare adottando misure tecniche e organizzative adeguate atte a dare seguito alle richieste di esercizio dei diritti da parte degli interessati di cui al capo III del Regolamento [...]

Nell'accordo tra Titolare e Responsabile sarà essenziale definire le modalità tramite le quali il responsabile supporterà il Titolare nel rispetto degli obblighi relativi al controllo sull'effettiva applicazione delle misure di sicurezza richieste, alla notifica di eventuali violazioni al garante o ai diretti interessati e alla valutazione d'impatto per la protezione dei dati.

[Riferimento al DPA] Rispettivamente i punti 2.11, 2.12, 2.13

Altro elemento da definire è cosa il Responsabile debba fare dei dati al termine del rapporto, infatti il Titolare dovrebbe indicare nel contratto o altro atto giuridico concluso con il responsabile se al termine del rapporto tra le parti i dati debbano essere cancellati fornendo idonea prova o certificazione dell'avvenuta cancellazione oppure questi vadano restituiti al Titolare e cancellati.

[Riferimento al DPA] Punto - 2.16 Termine del rapporto

Al termine della prestazione dei servizi che comportano l'attività di trattamento, il Responsabile dovrà:

- restituire i dati personali al Titolare del Trattamento ed eliminarli dalla propria infrastruttura informatica ed archivi cartacei, fornendo al Titolare idonea dichiarazione scritta dell'avvenuta distruzione dei dati.
- eliminarli in maniera permanente dalla propria infrastruttura informatica ed archivi cartacei, fornendo al Titolare idonea dichiarazione scritta dell'avvenuta distruzione dei dati.

Possiamo infine accennare agli obblighi spettanti al Titolare il quale ha l'obbligo di istruire in maniera precisa e dettagliata il Responsabile sulle modalità e le finalità del trattamento dei dati oggetto dell'accordo, di garantire il rispetto dei diritti degli interessati e di garantire che i dati siano stati raccolti in maniera lecita, per finalità determinate, che i dati siano adeguati, pertinenti e limitati a quanto necessario per il perseguimento delle finalità per cui sono raccolti.

5.9 —— Sistema documentale per la data protection

Nel presente paragrafo si riportano le principali indicazioni necessarie per la verifica di adeguatezza, in termini di completezza ed aggiornamento, del sistema documentale privacy che ogni organizzazione che tratta

dati personali, sia essa pubblica che privata, si trova a dover gestire per ottemperare agli adempimenti previsti dalla normativa in materia di protezione dei dati personali (da ultimo il GDPR).

Quanto di seguito riportato è suddiviso in due sezioni:

1) **ruoli e responsabilità**: vengono indicati i ruoli e le principali responsabilità delle figure coinvolte nella gestione del sistema documentale privacy;
2) **modalità di gestione**: vengono riportate indicazioni di metodo per la gestione del sistema documentale privacy.

5.9.1 ——— Ruoli e responsabilità

Vengono di seguito delineati i ruoli e le responsabilità delle figure coinvolte nelle attività di tenuta, verifica ed aggiornamento del sistema documentale privacy.

Il Chief Information Officer, Chief Information Security Officer, Chief Confidentiality Officer devono contribuire a:

- mantenere aggiornato l'intero sistema documentale, compreso il Registro del Trattamento, e simili documentazioni di framework del sistema di governo della privacy all'interno di una organizzazione;
- comunicare mutamenti che richiedono un aggiornamento relativamente alla protezione logica dei dati e alla protezione fisica delle risorse;
- provvedere all'aggiornamento di cartelle condivise di archiviazione della documentazione in formato elettronico o all'aggiornamento ad es. di una piattaforma intranet dell'organizzazione;
- inviare la documentazione aggiornata al Titolare per la validazione ed approvazione formale.

I Responsabili del trattamento devono contribuire a:

- aggiornare, in conformità alle eventuali modifiche relative alle modalità di trattamento, la modulistica delle informative rilasciate ai soggetti interessati nella propria area di riferimento (ad. es. nell'ambito dell'area clinica, dell'area laboratori, della direzione amministrazione e risorse umane ecc.);
- comunicare alle figure preposte al governo del sistema documentale le modifiche relative alle modalità di trattamento nonché gli eventuali mutamenti organizzativi o tecnici avvenuti all'interno del propria area di responsabilità
- compilare ed aggiornare il Registro del Trattamento del Responsabile.

Il DPO deve contribuire a:

- rendere disponibile, ai fini dell'aggiornamento del sistema documentale, la pareristica resa al Titolare del trattamento, o ai Responsabili, che eseguono il trattamento in merito agli obblighi derivanti dal Regolamento, nonché i pareri emessi in merito alla valutazione d'impatto sulla protezione dei dati ai fini della loro archiviazione;
- condividere i verbali o altri documenti emessi e/o ricevuti nell'ambito della cooperazione con l'Autorità di controllo per le questioni connesse al trattamento ai fini della relativa archiviazione all'interno del sistema documentale;

- sorvegliare la corretta gestione e l'aggiornamento del sistema di gestione documentale in conformità alle previsioni del GDPR.

Il Titolare del Trattamento, ha il compito di:

- verificare ed approvare report, verbali di audit, il Registro del Trattamento ex art.30 del GDPR, e altra documentazione che attenga il sistema di governo della privacy all'interno della organizzazione;
- approvare gli aggiornamenti del sistema documentale;
- approvare ed emanare procedure, linee guida e policy attinenti alla protezione dei dati personali e alla riservatezza delle informazioni archiviate e trattate dalla organizzazione.

5.9.2 ——— Modalità di gestione

Strutturazione del sistema documentale privacy

Nell'ambito dell'esecuzione degli adempimenti prescritti dal GDPR in materia di protezione dei dati personali, le figure che si trovano a dover ottemperare a tali adempimenti redigono, modificano, aggiornano, cancellano e conservano una rilevante mole di documenti, sia essi in formato cartaceo che elettronico.

La specificità del contesto di riferimento, o l'uso di particolari dispositivi e tecnologie (ad. es. sistemi di videosorveglianza, biomentria ecc.) può richiedere altresì l'adozione e conservazione di particolari documenti o la tracciatura delle attività di trattamento o, al contrario, rendere necessaria una conservazione documentale limitata in un arco temporale ristretto (si pensi ad. es. alle videoregistrazioni degli accessi a sale d'aspetto ospedaliere accessibili al pubblico).

Con riferimento alla struttura del sistema documentale privacy, si riporta di seguito una griglia rappresentativa della struttura base di un albero documentale in materia di privacy.

Area	*Descrizione*
Gestione della documentazione privacy	*Procedure, policy, linee guida operative che disciplinano il sistema di governo dei dati personali, ivi inclusa la procedura che disciplina i documenti che fanno parte del corpus regolamentare*
Registro dei Trattamenti	*Censimento dei trattamenti, ambito del trattamento consentito, processi operativi e flussi di dati, etc.*
Registro degli strumenti elettronici di trattamento	*Mappa dell'infrastruttura tecnologica* *Topologia di rete* *Elenco delle applicazioni* *Elenco dei server e dei sistemi operativi* *Elenco dei data base*
Analisi dei rischi e valutazione degli impatti	*Reportistica delle analisi dei rischi sui trattamenti di dati personali* *Reportistica delle valutazione di impatto per i trattamenti di dati personali che presentano un rischio elevato*

Area	Descrizione	
Ruoli & Responsabilità	*Modello organizzativo DPO*	
	delibere degli organi di vertice	*delibere CDA o altri organi di vertice, Comitati privacy ecc.*
	atti di nomina e designazione	*DPO, co-titolarità, Responsabili per ogni area (ad es. direzione HR, direzione scientifica, direzione amministrazione, direzione ricerca ecc), Incaricati.*
	agreement & clausole contrattuali	*agreement e clausole standard ad es. per la gestione dei trasferimenti dei dati tra un laboratorio e un centro di ricerca, tra strutture sanitarie distinte ecc.*
Registro delle terze parti	*Mappa di tutte le terze parti cui sono affidati dei trattamenti o l'amministrazione dei sistemi e i relativi sub-fornitori* *DPA con le terze parti* *Evidenze di rispetto delle obbligazioni contrattuali, da parte delle terze parti*	
Misure di sicurezza	*documenti di regolamentazione*	*policy, regolamenti, linee guida, procedure, istruzioni operative, ex DPS se in uso o documenti simili, codici di condotta*
	misure di sicurezza tecniche	*policy tecniche, standard di riferimento, certificazioni tecniche (E.g. ISO 27001)*
	misure da provvedimenti specifici e generali del Garante o della PA di riferimento (ad es. Ministero di salute)	*provvedimenti generali del garante ad es. in tema di videosorveglianza, amministratori di sistema, dossier sanitario, fascicolo sanitario elettronico, banche dati PA ecc.* *Provvedimenti specifici del Garante*
Comunicazione e formazione	*comunicazioni interne*	*circolari, ordini di servizio, note di rilievo in mabito gestione documenti privacy e trattamenti*
	formazione	*corsi di formazione, evidenze della formazione ecc.*
Informative e Consensi	*pazienti in cura, in day-hospital, ricoveri, dipendenti, visitatori, familiari, consulenti, fornitori, altri*	
Registro delle Violazioni di sicurezza	*Registro di tutte le violazioni di sicurezza, valutate a rischio alto, notificate all'autorità Garante o agli interessati del trattamento*	
Esercizio dei diritti degli interessati del trattamento	*Registro delle richieste degli interessati del trattamento, in relazione all'esercizio dei diritti (limitazione, opposizione, cancellazione, accesso, rettifica, portabilità)*	
Accordi Sindacali	*Accordi sindacali in materia di internet e posta elettronica, videosorveglianza, amministratori di sistema, geolocalizzazione, biometria ecc.*	
Autorità Garante	*notificazioni, verbali ispezioni, richieste autorizzazioni, consultazioni*	
Rapporti di audit	*rapporti di Audit, report periodico sulla conformità agli adempimenti privacy, flussi informativi da/verso il DPO*	

Aggiornamento del sistema di gestione documentale privacy

Il sistema di gestione documentale privacy deve essere continuamente alimentato in virtù di novità originate da cambiamenti organizzativi o gestionali, dell'adozione di nuovi dispositivi o di nuove tecnologie, a fronte di novità normative, abrogazione di disposizioni legislative e provvedimenti dell'Autorità di controllo.

A tal fine, si consiglia un continuo monitoraggio per verificare se siano intervenute modifiche e/o novità di rilievo, ad es. relative alla protezione logica dei dati o alla protezione fisica delle risorse, tali da richiedere un aggiornamento dei documenti (ad es. dell'ex. DPS se in uso o altra documentazione attinente il governo della privacy, aggiornamento della modulistica relativa all'informativa e consenso ecc.).

Si descrive di seguito un possibile approccio operativo sequenziale per l'aggiornamento del sistema documentale privacy:

- analizzare i mutamenti organizzativi o normativi e valutare la necessità di aggiornare il sistema documentale privacy (a cura del CIO, CISO, DPO, DPM, ufficio legale e compliance e/o figure alle quali sono attribuite responsabilità in materia di privacy);
- in caso di valutazione positiva, procedere al suddetto aggiornamento;
- inviare l'aggiornamento al Titolare del trattamento per l'approvazione delle modifiche introdotte;
- collaborare con il Titolare nell'analisi del sistema documentale aggiornato nel caso in cui siano necessari chiarimenti circa le modifiche apportate;
- provvedere a rendere l'aggiornamento pubblico e disponibile agli interessati se previsto per legge (ad. es. mediante affissione nei locali accessibili al pubblico, pubblicazione nel sito web della azienda ospedaliera ecc);
- provvedere all'archiviazione legale dell'aggiornamento possibilmente conservando la tracciatura della data di ultimo aggiornamento.

Il DPO sorveglierà anche la corretta attuazione degli aggiornamenti del sistema documentale in conformità al Regolamento.

5.10 ——— Il sistema di monitoring

5.10.1 ——— Attività di monitoraggio

Il Regolamento attribuisce al Data Protection Officer (di seguito anche solo definito "DPO") il compito di assistere il Titolare e il Responsabile del trattamento nel controllo dell'effettivo funzionamento dei presidi posti in essere al fine di garantire la protezione dei dati personali.

Il DPO assume un **ruolo di vigilanza**, non deve altresì garantire la conformità alle prescrizioni del Regolamento. Dovrà, dunque, vigilare sull'effettivo rispetto della normativa del GDPR e di quella ulteriore specifica eventualmente vigente per il settore di riferimento.

In aderenza alle Linee guida del WP 29 sul DPO, adottate il 5 aprile 2017[25], oltre al compito di informare e fornire consulenza al Titolare/ Responsabile del trattamento in merito agli obblighi derivanti dal Regolamento, fornendo anche pareri, il DPO ha lo specifico compito di

monitorare

l'osservanza del GDPR

allo scopo di garantire la sicurezza dei trattamenti.

La posizione ricoperta dal DPO nell'ambito dell'organizzazione, sia pubblica che privata, deve pertanto garantire l'autonomia dell'iniziativa di controllo da ogni forma d'interferenza e di condizionamento da parte di qualunque componente dell'organizzazione stessa (e in particolare dei soggetti apicali).

Tale obiettivo si può ragionevolmente conseguire inserendo il DPO in una posizione "gerarchica" elevata e prevedendo il suo "riporto" direttamente al Consiglio di Amministrazione nel suo complesso (od altri tipi di organismi apicali corripondenti).

Per garantire la necessaria autonomia di iniziativa e l'indipendenza nella attività di monitoraggio e verifica è necessario, inoltre, che al DPO non siano attribuiti compiti operativi e comunque al di là delle funzioni ad esso espressamente attribuite dal Regolamento, ciò al fine di non minare l'obiettività di giudizio nel momento in cui opera la sorveglianza sulla conformità alla normativa vigente.

Inoltre, il DPO deve essere dotato di tutti i poteri necessari per assicurare un puntuale ed efficiente monitoraggio.

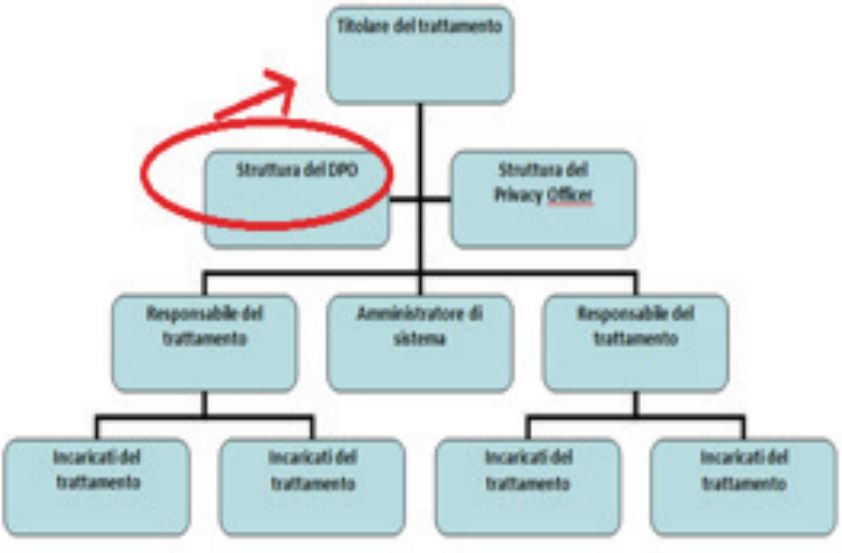


Figura: posizione di indipendenza e di riporto diretto al Titolare da parte del DPO - Fonte: Deloitte

25. Guidelines on Data Protection Officers ('DPOs') consultabili sul sito ufficiale del WP 29 al seguente link http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

5.10.2 ——— KPI di monitoraggio

Per agevolare le attività di monitoraggio e reporting in carico al DPO, può essere utile definire e implementare un sistema basato su opportuni KPI. Di seguito si riportano alcuni esempi di applicazione:

- KPI relativi al rispetto della normativa interna da parte degli attori coinvolti nei processi di Data Protection
- KPI relativi alle clausole contrattuali previste negli accordi di outsourcing
- KPI relativi al rispetto delle finalità di trattamento dei dati concordate
- KPI relativi al numero di incidenti relativi al trattamento dei dati
- KPI relativi al tempo impiegato per la comunicazione all'Autorità Garante di avvenuti data breach.

Nell'ambito della continua attività di monitoraggio della corretta applicazione del Regolamento, il DPO svolge in particolare le seguenti mansioni:

- **indirizza e coordina** le attività in materia di protezione dei dati personali;
- **controlla** che **le violazioni** dei dati personali siano documentate, notificate e comunicate internamente;
- assume (con il Titolare) il compito di **punto di contatto per l'autorità di controllo** per questioni connesse al trattamento e, se del caso, consulta l'autorità di controllo di propria iniziativa nel caso in cui sia necessario sottoporre quesiti o istanze di verifica;
- **interagisce con le figure** a presidio tecnico e fisico in materia di protezione dei dati personali.

5.10.3 ——— Flussi informativi da parte del DPO

Compito precipuo del DPO è quello di segnalare all'organo dirigente (ovvero al Titolare del trattamento), per gli opportuni provvedimenti, quelle violazioni accertate che possano comportare l'insorgere di una responsabilità in capo all'organizzazione per non conformità al Regolamento.

Il rapporto con gli organi apicali deve essere su base continuativa: il DPO dovrebbe, pertanto, instaurare flussi informativi, con cadenza regolare, per l'organo dirigente.

A titolo esemplificativo, il flusso informativo dal DPO verso il Titolare (a seconda dei casi CDA, Collegio sindacale, Organismi di Vigilanza ecc.) potrebbe avere ad oggetto:

- informazioni dettagliate sul livello di adeguatezza della sicurezza e della capacità di prevenzione di trattamenti in violazione del Regolamento;
- evidenze di ipotesi di trattamento a "rischio elevato" (ad es. introduzione di sistemi di trattamento di categorie particolari di dati di soggetti particolarmente vulnerabili, carenza di efficacia di misure a fronte di intervenuti cambiamenti organizzativi o tecnici ecc.);
- istanze da presentare all'Autorità di controllo;
- ispezioni in loco da parte dell'Autorità di controllo;
- particolari criticità attinenti la protezione dei dati personali, nell'ottica del principio di accountability, emerse a seguito di segnalazioni esterne o interne alla organizzazione.

In linea di massima, le attività di monitoraggio e verifica poste in essere dal DPO non dovrebbero essere sindacate da alcun altro organismo o struttura dell'organizzazione, dovendo avere altresì libero accesso presso

tutte le aree della organizzazione, senza necessità di alcun consenso preventivo, onde ottenere ogni informazione o dato ritenuto necessario per lo svolgimento dei suoi compiti di monitoraggio.

5.10.4 ——— I molteplici protagonisti del sistema di monitoraggio

Oltre all'attività del DPO, vi sono altri attori interessati al monitoraggio della corretta gestione privacy all'interno di una organizzazione, essi sono in generale:

- il Chief Information Security Officer (CISO): figura di riferimento responsabile di implementare programmi di protezione e mettere in campo processi volti a mitigare i rischi, alla luce della politica di gestione del trattamento del DPO;
- il Responsabile Sicurezza Fisica (Physical Security): figura di riferimento per la gestione della sicurezza fisica di una organizzazione (ad es. circa il corretto uso di dispositivi);
- i Responsabili del Trattamento: responsabili nominati eventualmente dal Titolare in ragione delle specifiche aree di competenza (ad es. il direttore sanitario, il direttore risorse umane, il direttore scientifico ecc);
- i Data Processing Manager (DPM): individuati dal Responsabile del trattamento per la propria area di responsabilità, sono figure delegate alle attività di presidio e governo delle operazioni di trattamento effettuate dal personale che opera all'interno delle proprie aree/direzione (es. capo reparto, responsabile infermeria, responsabile ufficio rapporti con il pubblico ecc.);
- gli Amministratori di Sistema: figure alle quali si attribuisce l'incarico di gestire e manutenere un impianto di elaborazione dati o di sue componenti;
- gli Incaricati del trattamento: tutte le risorse che, a prescindere dalla direzione di appartenenza dal ruolo ricoperto o dall'inquadramento contrattuale, svolgono trattamenti sui dati personali (ad. es. medici che trattano dati dei pazienti, addetti all'ufficio risorse umane che trattano i dati dei dipendenti della struttura sanitaria, gli addetti ai laboratori che trattano dati genetici ecc.).

Va tenuto presente che, avendo il DPO una competenza ratione materiae, ossia sul rispetto del particolare ambito di normativa riguardante la protezione dei dati personali applicabile ad una organizzazione, esso risulta di conseguenza il destinatario privilegiato di ogni informazione utile a questo fine da parte degli ulteriori protagonisti della gestione privacy all'interno dell'organizzazione. Quest'ultimi, dal canto loro, essendo comunque investiti della responsabilità di valutare l'adeguatezza "in generale" dei presidi in materia privacy dovranno essere sempre informati di una eventuale non conformità rispetto al Regolamento, così come di eventuali carenze di presidi: in tal modo essi potranno attivarsi secondo quanto previsto dalla legge. Ciò garantisce un presidio coordinato delle operazioni di trattamento ed una responsabilità privacy coerente con l'effettivo ruolo ricoperto.

I flussi informativi attinenti le attività di monitoraggio, pertanto, oltre ad essere attivati da parte del DPO verso gli organi apicali dell'organizzazione, saranno altresì alimentati da parte dei suindicati soggetti coinvolti nella gestione della privacy verso il DPO. Il flusso informativo, pertanto, assumerà carattere bidirezionale.

A titolo esemplificativo, il flusso informativo verso il DPO da parte dei soggetti interessati nel sistema di governance in materia di data protection, potrebbe avere ad oggetto:

- segnalazione della introduzione di una nuova tecnologia;
- segnalazione di ipotesi violazioni interne da parte del personale dipendente;

- reportistica relativa a verifiche attinenti alle procedure di governo delle aree/direzioni di riferimento (reparti, uffici, laboratori, sale di accesso al pubblico ecc.);
- criticità nella protezione dei dati emerse nelle relazioni con pazienti, dipendenti o fornitori;
- istanze pervenute da parte dei pazienti;
- carenze di efficace del sistema di contrasto e mitigazione dei rischio registrate a fronte di audit svolti da team di internal audit o da parte di organismi di vigilanza;
- qualunque comunicazione ricevuta/inviata dalla Autorità di controllo.

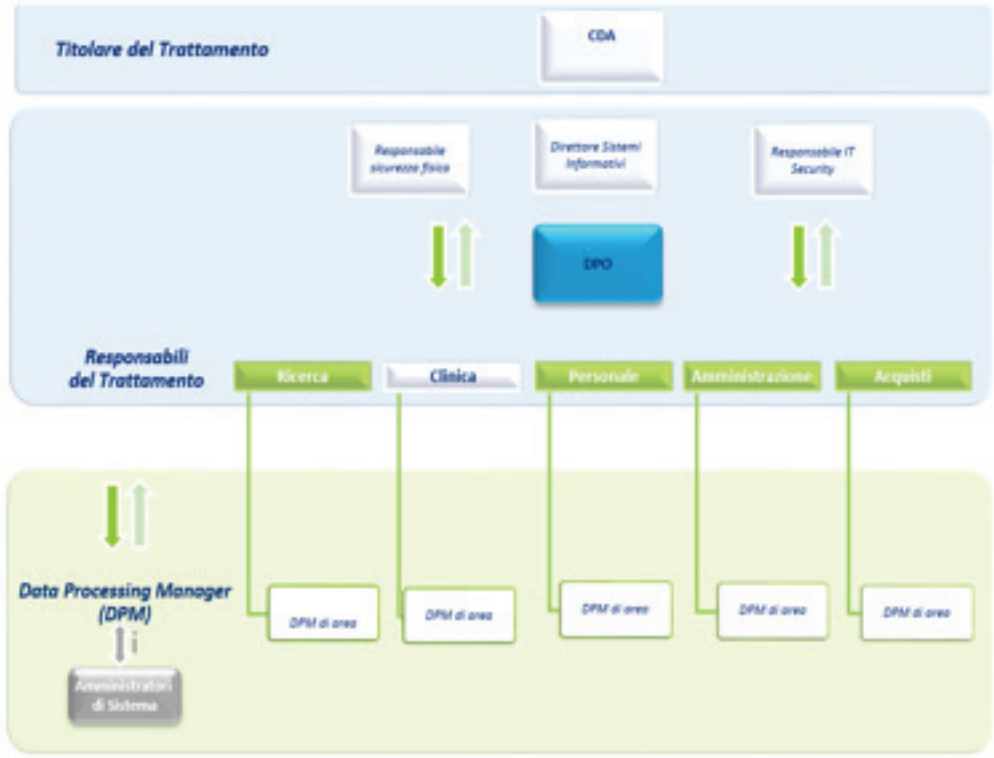


Figura: esempio di flussi informativi tra DPO, aree di governo e prime linee suddivise per area di competenza- Fonte: Deloitte

5.11 —— Data Breach

I dati personali conservati, trasmessi o trattati da organizzazioni sia nel settore privato che pubblico possono essere soggetti al rischio di perdita, distruzione o diffusione indebita, ad esempio a seguito di attacchi informatici, accessi abusivi, incidenti o eventi avversi, come incendi o altre calamità. Si tratta di situazioni che possono comportare pericoli significativi per la privacy degli interessati cui si riferiscono i dati.

Il GDPR prevede l'obbligo di **notifica all'autorità di vigilanza** in caso di violazione dei dati personali nonché la definizione di altri requisiti per l'eventuale ulteriore comunicazione ai soggetti interessati.
Tale obbligo non risulta del tutto nuovo, in quanto il Garante per la protezione dei dati personali aveva già adottato negli ultimi anni una serie di provvedimenti che introducono, per determinati settori, l'obbligo di comunicare eventuali violazioni di dati personali (*c.d. data breach*) all'Autorità stessa e, in alcuni casi, anche ai soggetti interessati, pena l'applicazione di sanzioni amministrative.

In particolare, si segnala il *Provvedimento del Garante privacy n. 331 del 4 giugno 2015 in tema di dossier elettronico*. Come noto, il **dossier sanitario elettronico** è lo strumento costituito presso un'unica struttura sanitaria (ospedale, azienda sanitaria, casa di cura) che raccoglie informazioni sulla salute di un paziente al fine di documentarne la **storia clinica** presso quella **singola struttura** e offrirgli un migliore processo di cura, differenziandosi dal **fascicolo sanitario elettronico** in cui invece confluisce l'intera storia clinica di una persona generata **da più strutture sanitarie.** Con il provvedimento succitato, il Garante per la protezione dei dati personali ha varato le linee guida che puntano a definire un quadro di riferimento unitario per il corretto trattamento dei dati raccolti nei dossier, già istituiti o che si intendono istituire, da parte di strutture sanitarie pubbliche e private.
In particolare, ai pazienti deve essere consentito di **scegliere**, in piena libertà, se **far costituire o meno il dossier sanitario**:

- in assenza del consenso il medico avrà a disposizione solo le informazioni rese in quel momento dal paziente o in precedenti prestazioni fornite dallo stesso professionista
- la mancanza del consenso non deve incidere minimamente sulla possibilità di accedere alle cure richieste
- sarà necessario un consenso specifico per poter inserire nel dossier informazioni particolarmente delicate (infezioni Hiv, interventi di interruzione volontaria della gravidanza, dati relativi ad atti di violenza sessuale o pedofilia)
- per consentire al paziente di scegliere in maniera libera e consapevole, la struttura sanitaria dovrà informarlo in modo chiaro, indicando in particolare, chi avrà accesso ai suoi dati e che tipo di operazioni potrà compiere.

A fronte dei diritti riconosciuti ai pazienti a cui apprestare la massima tutela, sono prescritti gli speculari obblighi posti in capo al Titolare del trattamento, tra i quali appunto rientra anche la notifica in caso di data breach. A tal proposito, il Garante ha stabilito che entro 48 ore dalla conoscenza del fatto, le strutture sanitarie pubbliche e private sono tenute a comunicare al Garante, tramite un modello reso disponibile sul sito web del Garante, all'indirizzo pec all'uopo predisposto, tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui dati personali trattati attraverso il dossier sanitario.

Tale disciplina andrà letta in coordinamento con le previsioni del GDPR in materia di notifica delle violazioni (ad. es. per quanto riguarda il termine di notifica).

Riferimenti Normativi

Artt. 33-34 Regolamento

1. In caso di violazione dei dati personali, il Titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.
2. Il responsabile del trattamento informa il Titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

3. La notifica di cui al paragrafo 1 deve almeno:
   a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
   b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
   c) descrivere le probabili conseguenze della violazione dei dati personali;
   d) descrivere le misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.
4. Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.
5. Il Titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo.
6. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.
7. La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d). […]

5.11.1 ——— La ratio

Il fondamento della previsione della notifica all'Autorità di controllo si rinviene nella volontà di affrontare e gestire nell'immediatezza una violazione, al fine di evitare l'insorgenza o l'aggravamento di danni materiali o immateriali alle persone interessate (perdita di controllo de dati, limitazione dei diritti dell'interessato, discriminazione, furto o usurpazione dell'identità, perdite finanziarie ecc.).

L'episodio pregiudizievole, pertanto, non deve mai essere celato poiché l'oscuramento della notizia può amplificare gli effetti negativi dell'evento dannoso e inibire forme di intervento dell'Autorità di controllo così come dell'interessato i cui dati sono stati violati.

5.11.2 ——— In cosa consiste l'attività di notifica

Il Titolare del trattamento deve notificare all'Autorità di controllo una violazione di cui è venuto a conoscenza **appena possibile e comunque entro 72 ore** da quando ha avuto cognizione dell'accaduto. Tale notifica **non è obbligatoria se** il Titolare abbia valutato che **sia improbabile che la violazione dei dati personali di cui è venuto a conoscenza presenti un rischio per i diritti e le libertà delle persone fisiche**.

La **notifica tardiva** (dopo 72 ore dall'avvenuta conoscenza della violazione) è ammessa dal GDPR che però richiede al Titolare l'onere di indicare esattamente i motivi del ritardo. Altresì, qualora non sia possibile per

il Titolare fornire tutte le informazioni utili contestualmente alla prima segnalazione della violazione, il GDPR consente allo stesso di fornirle in fasi successive senza ulteriore ingiustificato ritardo.

5.11.3 ——— Contenuto della notifica

Il contenuto della notifica è indicato espressamente dal GDPR che richiede la descrizione:

- della natura della violazione dei dati personali, categorie, numero di interessati: occorrerà dettagliare e circostanziare quanto più possibile la violazione rilevata (ad es. indicare quando è avvenuta se si ha contezza della data precisa o se sia ancora in corso di svolgimento, dove si è verificata nel caso di smarrimento o furto di dispositivi);
- dell'identità del Responsabile della protezione dei dati (DPO) o di un altro punto di contatto (è opportuno indicare riferimenti utili per una effettiva e tempestiva reperibilità quali mail/pec, recapiti telefonici, sede ecc.)
- della conseguenze della violazione (possibili danni stimati in termini di probabilità);
- delle misure proposte o adottate dal Titolare per porne rimedio.

Al fine di fornire una descrizione quanto più precisa della violazione, si consiglia di circostanziare la descrizione della violazione facendo riferimento alle informazioni elencate nella tabella di seguito riportata:

Indicazioni circa la violazione percepita	Lettura Copia Alterazione (i dati sono presenti sui sistemi ma sono stati alterati) Cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione) Furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione) …Altro
Indicazioni circa il dispositivo oggetto della violazione, con indicazione della ubicazione	Computer Rete Dispositivo mobile File o parte di un file Strumento di backup Documento cartaceo ...Altro
Indicazioni circa il tipo di dato oggetto di violazione se già individuabile nello specifico al momento del rilevamento della violazione	Dati anagrafici Indirizzo di posta elettronica Dati di accesso e di identificazione (user name, password, customer ID, altro) Dati idonei a rivelare lo stato di salute Dati relativi a minori Dati sanitari relativi a persone sieropositive, a donne che si sono sottoposte a un'interruzione volontaria di gravidanza, a vittime di atti di violenza sessuale o di pedofilia, a persone che fanno uso di sostanze stupefacenti, di sostanze psicotrope e di alcool, a donne che hanno deciso di partorire in anonimato, i dati riferiti ai servizi offerti dai consultori familiari Copie per immagine su supporto informatico di documenti analogici …Altro

Infine, il Titolare del trattamento deve essere in grado di documentare qualsiasi violazione dei dati personali, comprese le suindicate circostanze a essa relative, oltre che le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione deve consentire all'Autorità di controllo di verificare il rispetto delle prescrizioni previste nel GDPR.

5.11.4 ——— Processo complessivo di data breach management

È necessario chiarire come un completo piano di data breach management non possa limitarsi alla sola fase di violazione e successiva gestione dei breach, ma sia un processo che parte fin dalla fase di ingresso dei dati nella struttura del Titolare/Responsabile, passa attraverso la fase di mappatura, prosegue tramite l'adozione di adeguate misure di sicurezza, e si conclude con l'eventuale notifica all'autorità Garante e/o con la comunicazione agli interessati.

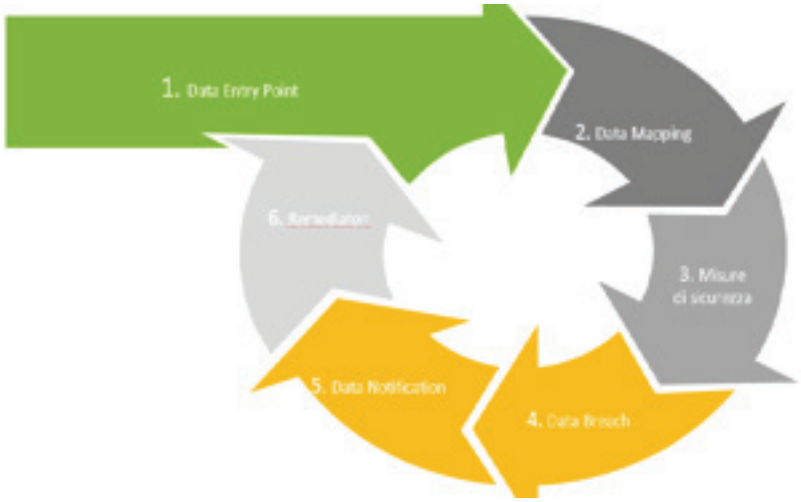


Figura: flusso complessivo di data breach management - Fonte: Deloitte

In linea con l'ottica di interpretare un piano di data breach management quale "**processo complessivo**", che deve avviarsi sin dal momento della raccolta dei dati all'interno della struttura del Titolare, è bene evidenziare come debbano essere visti come strettamente dipendenti gli aspetti riguardanti "il Monitoraggio del Sistema Complessivo di Sicurezza" (*Monitoring*) e di "gestione della Violazione della Sicurezza delle Informazioni" (*Data Breach*).

In particolare, **controlli insufficienti a riguardo della divulgazione delle informazioni** possono aumentare la probabilità di informazioni condivise in modo inappropriato. Inoltre, il contesto in cui vengono utilizzate o divulgate le informazioni può cambiare nel corso del tempo, portando queste ultime ad essere utilizzate per scopi diversi senza che le persone (soggetti che hanno fornito consapevolmente l'informazione in sè stessa o l'autorizzazione a raccogliere l'informazione che li riguarda quale conseguenza di azioni pertinenti e necessarie allo scopo dichiarato per cui l'informazione stessa è raccolta) ne siano a conoscenza.
Da ciò possono configurarsi azioni intrusive rispetto alla sicurezza, libertà e diritti della persona o anche lesive della reputazione personale.

Pertanto, qualora una violazione della sicurezza delle informazioni, in un dato contesto, **sembri apparentemente non significativa**, la stessa può essere parte di un **insieme più vasto di azioni** che, viste in ottica di interrelazione più ampia, possono creare nell'insieme pregiudiziali di "Rischio Elevato".

Oltre alle necessarie notifiche, in attuazione di un piano complessivo di data breach management, è fondamentale che **venga riconsiderata la capacità complessiva da parte dell'Ente / Azienda / Struttura** di trattare e conservare in modo sicuro tutte le informazioni in suo possesso, anche se queste sono nativamente acquisite e trattate in forma disgiunta.

Infine, dal punto di vista organizzativo, andrebbe posta attenzione su una eventuale:

- *"eccedenza di trattamento"*,ovvero dati inutilmente raccolti e memorizzati
- *"conservazione oltrelimite"*, quando i dati sono conservati per più tempo di quanto sia necessario
- *"utilizzi impropri"* per lo svolgimento delle mansioni -cd.Insider Threat-, quando vengono utilizzate o divulgate le informazioni per scopi diversi da quelli per cui sono state raccolte (esempio: un medico fornisce l'elenco dei propri pazienti al fratello che si occupa della commercializzazione di presidi medici).

5.11.5 ——— La valutazione dell'impatto di una violazione

La valutazione del rischio è finalizzata a quantificare la "magnitudo" delle conseguenze del data breach, ovverosia del danno, patrimoniale e non patrimoniale, derivante dalla violazione dei dati personali.

La combinazione di probabilità e gravità consente di stimare il potenziale rischio per i diritti e le libertà delle persone fisiche, e così valutare se procedere o meno con la notificazione all'Autorità Garante e/o agli interessati coinvolti.

A tal proposito, oltre a rimandare alle generali considerazioni relative alle attività di valutazione riportate nella sezione "Analisi preliminare del rischio", si riporta di seguito uno schema di riferimento circa l'attivazione degli adempimenti di notifica e comunicazione a seguito della valutazione effettuata:

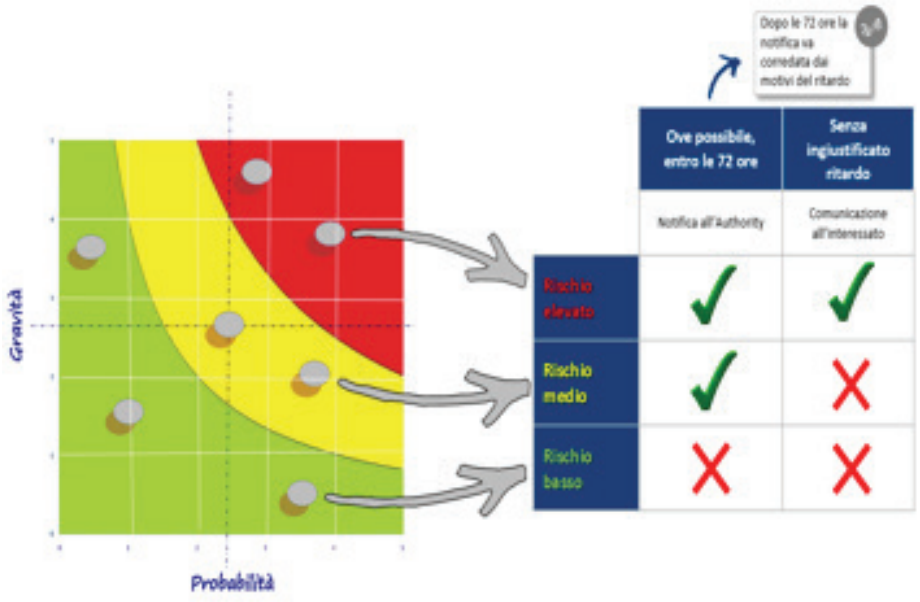


Figura: attivazione degli adempimenti di notifica e comunicazione - Fonte: Deloitte

5.11.6 ——— Ulteriori comunicazioni al soggetto interessato

Relativamente alla notifica verso gli interessati, il Titolare secondo il GDPR deve notificare la violazione anche all'interessato i cui dati personali sono stati oggetto della violazione rilevata senza ingiustificato ritardo e in modo chiaro solo in un caso: qualora la violazione dei dati rischi di **pregiudicare i diritti e le libertà dell'interessato**.

Le ragioni di tale comunicazione si rinvengono nel fatto che, in caso di eventuali pregiudizi, il soggetto interessato deve essere posto nelle condizioni di prendere le **precauzioni necessarie**.

La comunicazione, invece, non dovrebbe essere necessaria in tutti i casi in cui il Titolare **valuta che non può derivare un danno** materiale o immateriale dalla violazione, in particolare:

- quando il Titolare si era già dotato di misure tecniche e organizzative adeguate alla protezione dei dati personali soprattutto rendendoli incomprensibili (cifratura);
- quando il Titolare è in grado di dimostrare di aver attuato successivamente specifiche misure per la gestione del rischio elevato per i diritti e le libertà dell'interessato.

Inoltre, la comunicazione agli interessati non è dovuta secondo il GDPR quando implicherebbe **uno sforzo sproporzionato**. In tal caso, naturalmente, il Titolare non è esentato dall'obbligo ma può optare per una forma diversa dalla comunicazione individuale, avvalendosi di una **comunicazione pubblica** (o misura simile) che garantisca, comunque, analoga efficacia per i soggetti interessati (ad. es inserzione su un quotidiano, comunicazione evidente sulla home page del sito web del Titolare ecc.).

Rispettare i requisiti normativi, avrà impatti significativi di natura tecnologica, di processo ed organizzativi per le organizzazioni operanti nel settore sanitario che trattano dati ad alta sensibilità. In particolare sarà necessario:

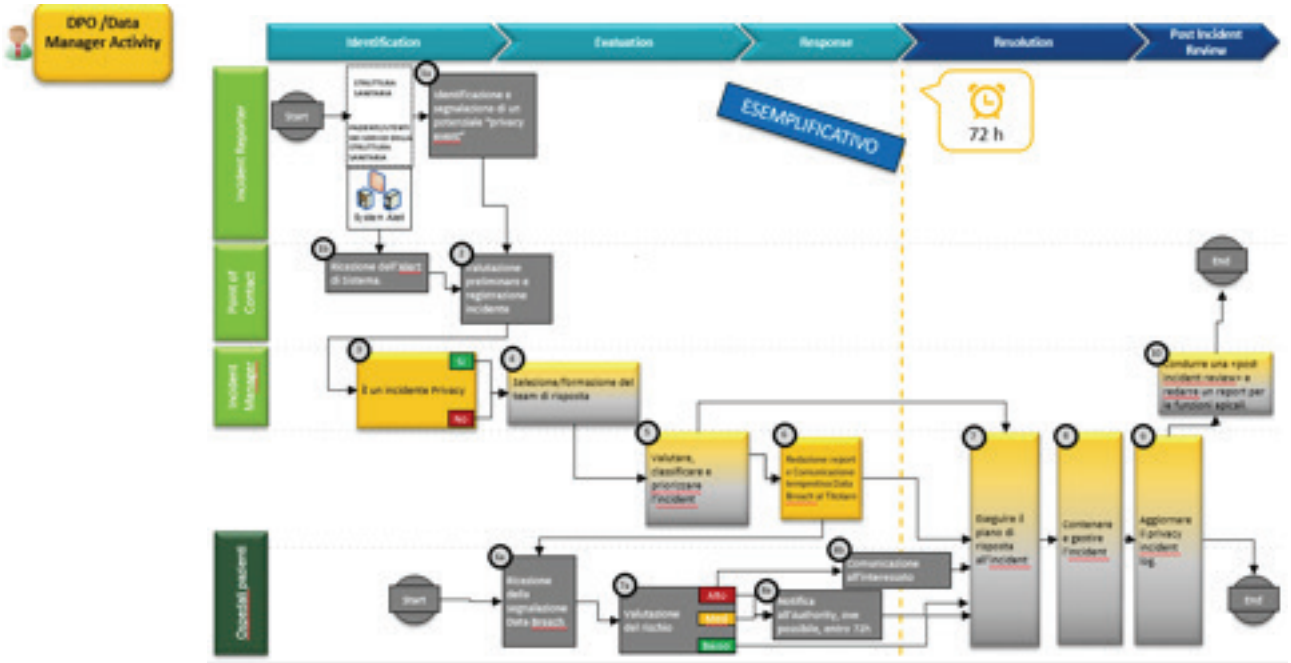
- identificare le classi di incidenti oggetto di valutazione (es. tassonomia);
- identificare il perimetro di sistemi contenenti dati personali dei pazienti;
- identificare referenti di aerea/direzione in grado di poter segnalare, analizzare e valutare gli incidenti tempestivamente e definire nuove responsabilità organizzative;
- identificare la data di attestazione in cui viene accertata la violazione e da cui sono misurate le tempistiche previste dalle normative.
- definire parametri di valutazione delle violazioni;
- identificare i referenti di area/direzione deputati alle comunicazioni verso i pazienti e l'Autorità;
- definire una procedura organizzativa di gestione delle violazioni dei dati;
- rafforzare il sistema di controllo di sicurezza per la mitigazione del rischio di possibili violazioni dei dati.

Infine, sarebbe opportuno coordinare le disposizioni del Regolamento con la disciplina prevista dal Garante privacy in merito a casi di data breach di sistemi biometrici nonché di banche della PA (anche in ragione delle prescritte specifiche misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche) peraltro in fase di adeguamento.

5.11.7 ——— Esempio di flusso di gestione

Di seguito di riporta, a titolo esemplificativo, un diagramma di flusso che descrive, secondo una logica di alto livello, un possibile **processo per gestire ipotesi di violazioni o c.d. privacy incident**.

Tale processo, naturalmente, dovrà essere integrato da tutte le necessarie procedure interne adottate dalla struttura sanitaria che regolamentino la gestione degli incidenti.



6 —— Le misure tecniche

Per affrontare in modo organico la gestione dei requisiti posti dal GDPR sul sistema informativo, non è sufficiente pianificare interventi puntuali di adeguamento. È necessario invece che la conformità diventi parte strutturale delle modalità di gestione ed evoluzione del sistema informativo. Laddove i sistemi e i processi di gestione presentino delle difficoltà oggettive all'adeguamento, questo può essere un elemento da valutare, nell'ottica di considerare "i costi di attuazione" degli adeguamenti. In conseguenza di tali costi e nella natura e dei rischi dei trattamenti, nonché del tipo di non conformità, in alcuni casi l'adeguamento potrà non essere immediato, ma dilazionato o diluito nel tempo. Viceversa, difficilmente queste considerazioni permetteranno di perseverare nella realizzazione o acquisizione di sistemi non conformi. Un esempio importante riguarda il tema della pseudonimizzazione. Introdurre la pseudonimizzazione nei processi e nelle applicazioni esistenti, come vedremo, può essere estremamente complesso. Tuttavia, i principi di privacy by design e by default richiamati più volte nel Regolamento, come anche il principio di necessità, ci dicono di trattare dati non pseudonimizzati solo quando strettamente necessario, ovvero quando l'associazione a dati identificativi è necessaria per il trattamento. Integrare questo tipo di protezione deve quindi diventare parte della normale progettazione dei sistemi. Per ridurre la complessità della gestione della pseudonimizzazione, e naturalmente per minimizzare il rischio di errori nell'associazione ai dati identificiativi (tema particolarmente critico e sentito nell'ambito sanitario), è opportuna una gestione per quanto possibile unica e centralizzata dell'anagrafe degli interessati. Questo è un esempio, fra i tanti, in cui l'evoluzione verso gestioni centralizzate di molti aspetti è necessaria, e corrisponde anche a quelle che sono considerate in generale buone pratiche nella progettazione e gestione dei sistemi. Altri casi significativi sono quello dell'autenticazione e della gestione dei profili di accesso.

In generale, sono diversi i temi che richiedono attenzione nella pianificazione di un adeguamento del sistema informativo che sia efficace e sostenibile nel tempo. Nel seguito saranno analizzati quelli principali. Naturalmente, sarà discusso un approccio ideale al quale le aziende dovranno tendere. In funzione dello stato attuale, delle risorse attuali e delle complessità specifiche, potranno trovare più o meno complesso raggiungere questo obiettivo.

6.1 —— Data protection by design

L'articolo 25 del GDPR si compone di due importanti commi le cui parti salienti possono essere cosi riassunti: *Comma 1) (concetto di protezione dei dati by design)……sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso* ***il Titolare del trattamento mette in atto misure tecniche e organizzative adeguate****, quali la pseudonimizzazione,* ***volte ad attuare in modo efficace i principi di protezione dei dati****, quali la minimizzazione,* ***e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.***

Comma 2) (concetto di privacy by default)…Il Titolare del trattamento mette in atto misure tecniche ed organizzative adeguate per garantire che siano trattatati, per impostazione predefinita, solo i dati personali per ogni specifica attività di trattamento…

In estrema sintesi al Titolare è richiesto di pensare di mettere in atto tutte le misure che consentano ad un trattamento di essere conforme al Regolamento e - come componente della accountability - di documentare tutto ciò che si è pensato di mettere in atto, le valutazioni che hanno portato a tali scelte, le evidenze che ne testimoniano l'implementazione (comma 2), come pure viene richiesto a Titolare o al Responsabile a cui sia affidata la gestore/realizzazione delle attività di trattamento di predisporre sin dal momento della progettazione (identificazione dei mezzi) sia al momento dell'erogazione dei servizi (atto del trattamento) misure adeguate quali ad esempio le condizioni di pseudonimizzazione e minimizzazione applicate ai dati stessi. In particolare quindi, se all'interessato è lasciata facoltà di scelta relativamente al trattamento dei dati personali, il responsabile del trattamento garantisce che siano trattati, di default, (**privacy by default appunto**) solo i dati personali necessari per ciascuna finalità specifica del trattamento e che, in particolare, la quantità dei dati raccolti e la durata della loro conservazione non vadano oltre il minimo necessario per le finalità perseguite. In particolare detti meccanismi garantiscono che, di default, non siano resi accessibili dati personali a un numero indefinito di persone e che gli interessati siano in grado di controllare la distribuzione dei propri dati personali.
Nell'ambito della normativa afferente alle pubbliche amministrazioni, e soprattutto per quanto riguarda l'interscambio di dati sanitari, sempre dettato da normative e vincoli istituzionali, alcuni dei concetti della privacy by default, legati particolarmente ai principi di *pertinenza e non eccedenza* si possono già trovare presenti nel provvedimento del Garante Privacy Italiano "Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche - 2 luglio 2015"
In particolare nella sezione 2.2 dell'allegato 2 di tale provvedimento sono presenti una serie di indicazioni molto bene definite sulle modalità di selezione dei dati da interscambiare:
La selezione delle informazioni personali oggetto di accesso deve avvenire nel rispetto dei principi di pertinenza e non eccedenza in relazione a ciascuna delle finalità perseguite dal fruitore. Rispetto ad una medesima banca dati devono essere, infatti, prefigurati diversi livelli e modalità di accesso che offrano al fruitore unicamente i dati necessari per le proprie esigenze istituzionali.
Le modalità di accesso alle banche dati devono essere, pertanto, configurate offrendo un livello minimo di accesso ai dati, anche limitando i risultati delle interrogazioni a valori di tipo booleano (ad es., web services che forniscono un risultato di tipo vero/falso nel caso di controlli sull'esistenza o sulla correttezza di un dato oggetto di autocertificazione). Livelli di accesso gradualmente più ampi possono essere autorizzati soltanto a fronte di documentate esigenze del fruitore da indicare in convenzione.
È chiaro, inoltre, che per ciascun fruitore possono essere individuate più modalità di accesso ad una medesima banca dati in relazione alle diverse funzioni svolte dai propri operatori per il perseguimento della medesima finalità, modulando così il livello di accesso ai dati. L'erogatore deve, infatti, far sì che sia consentita, per quanto più possibile, la segmentazione dei dati visualizzabili al fine di rendere consultabili dall'utente, anche in base al proprio profilo e in relazione al bacino di utenza del fruitore, esclusivamente i dati necessari rispetto alle finalità in concreto perseguite. In altri termini la convenzione deve prevedere l'accesso alle sole

informazioni pertinenti e non eccedenti rispetto alla finalità istituzionale perseguita dalla convenzione stessa. Particolare attenzione deve essere prestata, inoltre, nella scelta delle informazioni richieste per l'interrogazione diretta della banca dati, ovvero per l'invocazione dei web services, imponendo un set minimo di dati per l'individuazione puntuale del soggetto cui si riferiscono. Salvo eccezioni rigorosamente motivate e documentate nella convenzione, la risposta fornita all'interrogazione non deve, poi, contenere un elenco di soggetti.

Il concetto di **Privacy by Design** parimenti non è nuovo, in quanto nasce oltre 20 anni va, come idea della Dr. Ann Cavoukian, Privacy Commissioner dell'Ontario. L'idea è stata successivamente ripresa e fatta propria dalla 32a Conferenza Internazionale dei Garanti privacy tenutasi a Gerusalemme nel 2010 che al riguardo hanno rilasciato una risoluzione

I principi previsti dalla metrodologia della privacy by design sono molto semplici:

- prevenire e non correggere i problemi o le minacce relative alla privacy prima che si trasformino in un reale danno per la privacy;
- definire gli aspetti della privacy in tutte le fasi della valutazione dei rischi;
- garantire la sicurezza durante tutto il ciclo del prodotto o servizio, dalla pianificazione all'implementazione, all'azione ed al controllo attraverso la pianificazione, l'implementare e la garantire del controllare della sicurezza dei dati;
- il sistema deve adeguarsi all'utente garantendone la centralità;
- trattamento dei dati personali, consentendo l'accesso solo ai dati strettamente necessari;
- detenzione dei dati per il periodo strettamente necessario;
- creazione di dati non direttamente riconducibile alla persona attraverso la pseudonimizzazione;
- adozione di processi di Hardening, Vulnerability Management, Data Masking e Internal auditing

Ai fini pratici le Aziende Sanitarie per l'applicazione del regolamento Privacy dovrebbero richiedere a tutti i propri fornitori a cui affidano lo sviluppo di soluzioni e prodotti che questi ultimi forniscano, apposita dichiarazione relativa all'applicazione del principio del privacy by design su quanto costituente oggetto di sviluppo in base ai principi sopra esposti. In particolare le aziende ai fini di accountability devono richiedere dichiarazioni al fornitore che dovranno riportare:

- l'attestazione dell'avvenuta analisi del prodotto sulla base delle specifiche della GDPR;
- la sussistenza di apposita documentazione atta a dimostrare l'analisi di adeguatezza del prodotto rispetto alle prescrizioni normative;
- la disponibilità di predetta documentazione in caso di controllo dell'Autorità competente presso il Cliente.

I principi di protezione by default, si esplicano inoltre anche attraverso le azioni dei singoli incaricati che devono ovviamente nelle loro attività di trattamento dei dati applicare vincoli di minimizzazione delle informazioni inibire tutto ciò che non è necessario; di conseguenze per il controllo delle misure è importante che le aziende sanitarie identifichino figure preposte (es. DPO) per la pianificazione ed attuazione di processi di controllo periodico edi audit interni per verificare che i processi siano rispettati.

6.2 ——— Identità e accesso

Il GDPR contiene vari riferimenti alla necessità e all'impiego di soluzioni di Identity & Access Management. Ma come per molti altri aspetti di questo regolamento, i riferimenti non sono quasi mai espliciti. Non si troveranno, infatti, espressioni tipo "è obbligatorio, per proteggere i dati personali, l'utilizzo di sistemi Identity & Access Management "

D'altro canto però analizzando l'art. 5 "**Principi applicabili al trattamento di dati personali**" comma 1 paragrafo f)

"1. I dati personali sono: (C39)

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);

b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»);

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);

d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);

e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);….

f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza») "

e scorrendo l'art. 32 **Sicurezza del trattamento (C83)** al comma 1 capoverso d) e comma 2

"1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il Titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

a) la pseudonimizzazione e la cifratura dei dati personali;

=> Articolo: 4

b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

3. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo.

4. Il Titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal Titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri."

sembra che una soluzione di Identity e Access Management possa ragionevolmente rispondere ai requisiti.

Allineare efficacemente le identità e i privilegi di accesso dei propri utenti alle policy aziendali è un controllo di sicurezza vitale al giorno d'oggi e non deve essere più considerato solo come un "tradizionale" processo IT.

Con la rapida adozione di soluzioni cloud o mobile e i programmi BYOD (bring your own device) i perimetri aziendali si stanno esponenzialmente allargando, facendo crescere i punti di ingresso alla rete e ai dati aziendali, che devono essere resi sempre più sicuri.
È proprio la governance delle identità che consente di ridurre il rischio di compromissione dei dati e diventa la linea di difesa principale per la protezione da frodi

Per cercare di ridurre il rischio di compromessione dei dati, devono essere valutate adeguate soluzioni di identity and access management che consentano di:

- Automatizzare i processi di gestione dei ruoli degli utenti, di gestione delle policy di accesso e di gestione dei rischi
- Applicare e rinforzare i corretti livelli di accesso per utenti in continuo mutamento
- Ricertificare regolarmente i diritti di accesso degli utenti con un elevato livello di precisione
- Rilevare e agire rapidamente in base alle violazioni dei criteri di sicurezza
- Le user dei dipendenti, dei medici, del personale infermieristico e dei pazienti, sono tra i principali punti di ingresso alle importanti risorse del sistema IT nell'helthcare

Le domande più critiche, anche ai fini legali, da porsi includono:

- Chi ha accesso e a quali risorse e perché?
- Quando è stato rilasciato l'accesso?
- Esistono rischi connessi con gli attuali diritti di accesso?

Gli utenti devono avere un accesso sicuro e accedere solo ai dati e alle applicazioni di cui hanno realmente necessità e per cui sono stati autorizzati.
Devono essere eseguiti controlli regolari per garantire che tali i diritti di accesso e i relativi privilegi non vengano violati.

Il personale dell'IT sanitario ha, di norma, familiarità con il provisioning delle user-id per l'accesso alle applicazioni e quindi, di conseguenza, ha familiarità con la gestione delle policy di sicurezza.
Tuttavia, gli auditor interni e i responsabili del business hanno scarsa comprensione del modo in cui tali ruoli sono correlati alle operazioni del business stesso.

Infatti coloro che gestiscono gli account non sono, di solito, coloro che sono demandati a decidere a quali informazioni gli utenti devono o meno accedere.
Di contro i responsabili di business, cioè coloro che decidono a quali informazioni gli utenti possono accedere, non hanno le competenze tecniche necessarie per definirlo sugli strumenti IT.

Le soluzioni di identity and access management possono aiutare a mantenere la sicurezza dei dati sensibili e a mantenere la compliance dell'organizzazione. Possono fornire informazioni preziose sugli account, i privilegi e i diritti di accesso, della vasta gamma di utenti. Colmando le lacune della protezione delle identità, le organizzazioni possono combattere le minacce di usi involontari non corretti e furti intenzionali.

È necessario raccogliere le informazioni sull'utente e dei suoi privilegi da una varietà di fonti, incluse le applicazioni di business, i sistemi delle risorse umane e le piattaforme di provisioning esistenti.

Una dashboard incentrata sui processi di business può aiutare l'organizzazione intera (personale IT, auditor e gli utenti di business) al fine di:

- Garantire i corretti diritti di accesso degli gli utenti alle applicazioni
- Evitare il rischio associato a privilegi eccessivi e non autorizzati
- Riesaminare periodicamente e ricertificare i diritti degli utenti per favorire l'incremento della sicurezza
- Rendere sicuri i sistemi sanitari allo scopo di identificare le potenziali violazioni della separazione delle responsabilità (SoD : Separation of Duty) per evitare che alcuni privilegi di accesso possano creare conflitti di interesse.

Bisogna mettere in condizioni le aziende di avere un monitoraggio delle eventuali violazioni SoD, in modo tale da rilevare facilmente i conflitti e gestirli attraverso i corretti workflow di certificazione e autorizzazione.
Come risultato, le organizzazioni hanno la possibilità di certificare che gli utenti dispongano dei corretti accessi e possono ridurre le violazioni e quindi abbassare il rischio da minacce interne.

Gli ambienti sanitari sono caratterizzati da una costante modifica ai gruppi di utenti. Pertanto è una sfida continua assicurare che i diritti assegnati rimangano attuali e appropriati.

Ad es.
Quando viene assunto nuovo personale, vengono rilasciate le utenze, con i corretti accessi in base ai ruoli e alle responsabilità, ma cosa accade quando un dipendente cambia reparto o lascia l'organizzazione? Chi si preoccupa di aggiornare o revocare l'utenza?
Si può verificare, in modo proattivo che i dipendenti non godano di diritti inutili?

L'accumulo dei privilegi di accesso nel tempo è conosciuto come "enitlement creep" - ed è un problema in aumento. L'"Enitlement creep" crea un aumento esponenziale della complessità della gestione delle identità e aumenta il rischio di compromissione dei dati.
Attraverso un migliore sistema di monitoraggio dei diritti e semplificando il processo di fornitura e revoca degli accessi le organizzazioni possono assicurare una corretta gestione degli stessi minimizzando i gap che possono portare a frodi.

Si dovrebbe quindi provvedere a dotarsi di soluzioni che automatizzino le task, amministrando le identità, le loro credenziali, gli account e i permessi di accesso attraverso l'intera vita dell'utenza
In questo modo si possono attivare le revisioni degli accessi e i processi di ricertificazione richiesti dai regolamenti sanitari, liberando risorse IT per altre attività.
Attraverso workflow automatizzati si possono riesaminare periodicamente le utenze e i loro privilegi così da controllare e tracciare lo stato, per esempio, degli ex dipendenti e assicurare che i loro account vengano disattivati in modo tempestivo.

6.3 ——— Encryption

La cifratura è uno dei meccanismi richiamati in più parti del GDPR come strumento per la protezione dei dati personali. Questo richiamo così frequente sottolinea come sia un meccanismo di cui ci si aspetta, almeno in prospettiva, un utilizzo diffuso e abituale. La ragione è chiara: la sottrazione di un dato cifrato presenta rischi enormemente minori per gli interessati, rispetto alla sottrazione di dati in chiaro.
Nel valutare gli strumenti da utilizzare nei diversi contesti, è necessario innanzitutto considerare quali minacce si vogliano contrastare. Ad esempio, i meccanismi di cifratura trasparenti a basso livello (dei dischi, dei database) aiutano a limitare l'esposizione dei dati in caso di sottrazione dei supporti fisici o di accesso a basso livello, mentre non sono efficaci per eventuali violazioni a livello applicativo, dove la trasparenza stessa del meccanismo lo rende inefficace. Se quindi può essere utile cifrare i dischi dei portatili, per evitare l'esposizione dei dati in caso di furto o smarrimento del portatile stesso (minaccia in generale significativa e uno dei maggiori generatori di Data Breach), è molto meno utile cifrare i dischi di un server in un datacenter, dove il tema dell'accesso diretto al disco o della sua sottrazione è, di norma, molto meno interessante per le misure di controllo degli accessi fisici al datacenter stesso. Per contro, anche nel caso dei datacenter, la cifratura a basso livello riduce la complessità in caso di dismissione di dischi o apparati guasti.

È utile ricordare che il GDPR non segue una logica di "misure minime", la cui implementazione permette di raggiungere la conformità a prescindere dalla "qualità" ed efficacia dell'implementazione. Segue invece una logica di riduzione del rischio, chiaramente indicata ad es. nell'art. 32. Quindi avere implementato meccanismi di cifratura dei dati non garantisce in sé la conformità, se non si sono contrastate efficacemente le minacce più rilevanti.

Sempre riguardo alla cifratura, è utile sottolineare come gli attacchi agli algoritmi crittografici siano piuttosto infrequenti, mentre molto più frequenti sono gli attacchi ai processi/meccanismi di gestione delle chiavi, ai difetti del software che implementa gli algoritmi crittografici, ed ai processi che utilizzano gli algoritmi crittografici. Nella scelta degli strumenti da adottare, si deve quindi in generale fare più attenzione a questi aspetti (ad esempio, dove sono memorizzate le chiavi e a come sono gestite), anziché focalizzarsi sulla scelta degli algoritmi o su chiavi particolarmente lunghe. In generale, fare riferimento alle buone pratiche indicate ad esempio per la cifratura delle connessioni https[26].

Nel considerare l'utilizzo della cifratura dei dati, dobbiamo considerare almeno tre ambiti:

- **Data at rest**, ovvero dove i dati sono conservati (database ecc.); è preferibile adottare strumenti che offrano nativamente opzioni flessibili di cifratura dei dati attraverso semplici meccanismi di configurazione, anziché utilizzare soluzioni proprietarie che rendono più complessa e quindi meno abituale la cifratura dei dati; anche per questo è preferibile utilizzare pochi repository di qualità, anziché distribuire i dati fra molti repository specifici di singole applicazioni
- **Data in transit**, ovvero la trasmissione dei dati; seppure sia in generale preferibile la cifratura, in alcuni contesti può essere preferibile avere il transito dei dati in chiaro, perché il beneficio di avere strumenti di monitoraggio del traffico (IDS/IPS, WAF, bilanciatori ecc.) è tale da giustificare questa scelta apparentemente meno sicura. In questi casi si avranno quindi degli apparati sui quali si attestano le comunicazioni cifrate con l'esterno del datacenter, mentre all'interno del datacenter, in cui si adotteranno comunque altre misure di sicurezza (monitoraggio, segregazione ecc.) si potranno avere, dove utile, delle comunicazioni in chiaro. Sicuramente, le buone pratiche non consentono ormai più in nessun contesto l'utilizzo di connessioni in chiaro per le attività di amministrazione del sistema informativo (telnet ecc.). Dove strumenti particolarmente elementari o vetusti supportino solo accessi in chiaro, si possono utilizzare meccanismi da una parte di segregazione delle reti, dall'altra di tunnel cifrati, per ridurre l'esposizione del traffico[27].
- **Altri ambiti di elaborazione del dato**, particolare attenzione deve essere posta ad esempio all'utilizzo di servizi in cloud, per i quali il controllo accessi è meno sotto controllo da parte dell'azienda

È bene comunque sempre ricordare che l'efficacia dei meccanismi di cifratura vede il suo limite nel fatto che comunque i soggetti abilitati (utenze, applicazioni) hanno in generale accesso al dato in chiaro o alle chiavi di cifratura, e quindi la loro compromissione comporta comunque l'accesso al dato in chiaro.

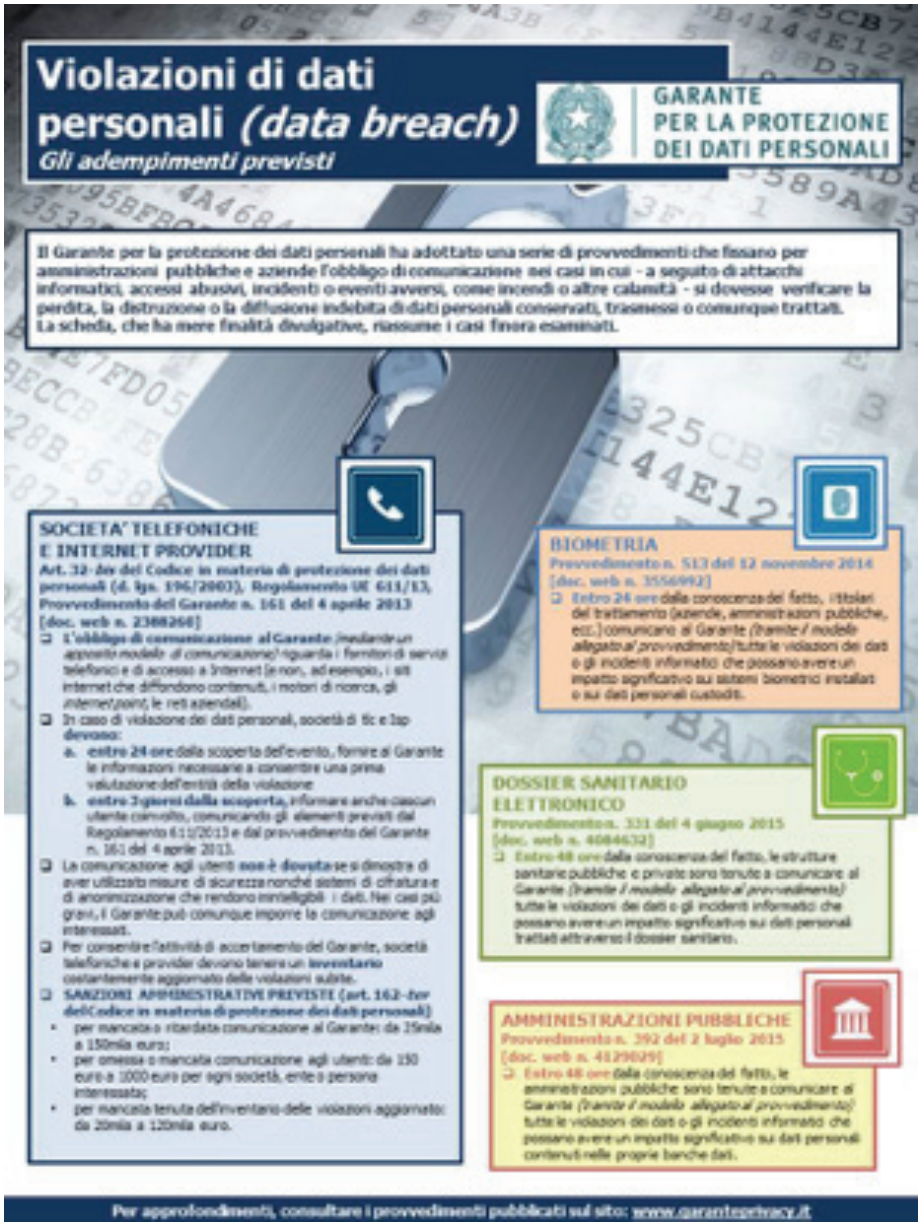
26. Vedi ad esempio https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet
27. Vedi ad es. per la gestione di PLC, https://www.certsi.es/en/blog/security-plc-updating ma comunque anche qui comincia ad essere supportato SSH, e questo supporto dovrebbe entrare nel tempo fra i requisiti per l'acquisizione di nuovi componenti.

6.4 ——— Logging e monitoraggio

L'art. 33 del Regolamento Europeo 679/2016 "Notifica di una violazione dei dati personali all'autorità di controllo" introduce nello scenario della sicurezza dei dati la necessità di notificare la violazione dei propri sistemi informatici (ossia un data breach) al Garante. Inoltre, l'art. 34 estende, in alcuni casi, tale notifica a tutti gli interessati.

Scatta, quindi, un obbligo di comunicazione: entro 72 ore da cui si viene a conoscenza di una violazione dei propri sistemi informatici è necessario seguire una procedura che notifichi la possibile violazione all'autorità Garante della Privacy.

Tale obbligo, che si estende quindi a tutti i titolari di trattamento di dati personali, non è comunque una novità per i quanto riguarda i servizi erogati in ambito di Pubblica Amministrazione ed in particolare il mondo della Sanità. Come è possibile verificare dall'infografica del Garante sul data breach, emessa nel 2015, che già il Provvedimento n. 513 del 12 novembre 2014 [doc. web n. 3556992 ed Provvedimento n. 392 del 2 luglio 2015 [doc. web n. 4129029] definivano le modalità ed i tempi di notifica (rispettivamente 24 e 48 ore) delle violazioni, nell'ambito del dossier sanitario e dell'interscambio dati tra le pubbliche amministrazione.



A prescindere quindi dall'eventuale adattamento o meno che potrà seguire a cura del Garante Privacy, rispetto modalità di comunicazione delle notifiche e della definizione univoca dei tempi, è sicuramente utile esaminare quanto riportato nelle raccomandazioni del Garante privacy pubblicate sul Sito www.garanteprivacy.it relative alle linee guida di implementazione del GDPR. Importante è la sottolineatura che la notifica deve avvenire soltanto se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati (si veda considerando 85). Pertanto, la notifica all'autorità dell'avvenuta violazione non è obbligatoria, essendo subordinata alla valutazione del rischio per gli interessati che spetta, ancora una volta, al Titolare. Se la probabilità di tale rischio è elevata, si dovrà informare delle violazione anche gli interessati, sempre "senza ingiustificato ritardo"; fanno eccezione le circostanze indicate al paragrafo 3 dell'art. 34, che coincidono solo in parte con quelle attualmente menzionate nell'art. 32-bis del Codice. I contenuti della notifica all'autorità e della comunicazione agli interessati sono indicati, in via non esclusiva, agli artt. 33 e 34 del regolamento. Su questo e su tutta la disciplina in materia, il Comitato europeo della protezione dati (si veda art. 70, paragrafo 1, lettere g) e h)) è chiamato a formulare linee-guida specifiche, alle quali sta già lavorando il Gruppo "Articolo 29".

Su questo tema ci sarà quindi da aspettarsi ulteriori approfondimenti. Ciò non toglie comunque che per quanto riguarda la gestione di incidenti in ambito sanitario, essendo l'informazione relativa allo stato di salute cittadino, una informazione il cui trafugamento è catalogata tra le situazioni che comportano alti rischi per i diritti e le libertà dell'interessato (considerando.75), essi ricadono sicuramente nell'ambito della notifica, a meno che non siano state prese delle misure tecniche (esempio crittografia o mascheramento di tutte le informazioni) che possano mitigare efficacemente conformemente al principio di responsabilizzazione che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.
Una ulteriore novità introdotta comunque dal GDPR in questo contesto è relativo alle sanzioni. Infatti, all'art. 83, comma 2, dove vengono elencati i fattori di cui l'autorità di controllo deve tenere conto nel determinare l'importo della sanzione, troviamo in particolare:

a) la natura, la gravità e la durata della violazione tenendo in considerazione la natura, l'oggetto o a finalità del trattamento in questione nonché il numero di interessati lesi dal danno e il livello del danno da essi subito;
b) il carattere doloso o colposo della violazione;
c) le misure adottate dal Titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati;

   …..(omissis).

f) il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi;

   …..(omissis).

h) la maniera in cui l'autorità di controllo ha preso conoscenza della violazione, in particolare se e in che misura il Titolare del trattamento o il responsabile del trattamento ha notificato la violazione;

   …..(omissis).

j) l'adesione ai codici di condotta approvati ai sensi dell'articolo 40 o ai meccanismi di certificazione approvati ai sensi dell'articolo 42;

È chiaro quindi che rilevare e notificare tempestivamente un incidente può limitare l'importo, potenzialmente molto elevato, delle sanzioni, e che viceversa non avere un sistema efficace di monitoraggio e rilevazione degli eventi e degli incidenti può aggravare la posizione dell'azienda in caso di data breach.

Per quanto riguarda la modulistica da compilare in caso di accertata violazione il Garante intende comunque rielaborare i modelli attualmente pubblicati.
Dal punto di vista delle azioni da mettere in campo gioca quindi un ruolo fondamentale da un lato l'applicazione delle misure di sicurezza (di cui si è già ampiamente discusso nel capitolo dedicato all'approfondimento dell'art 32 del GDPR), dall'altro la predisposizione di attività di log e di monitoraggio degli accessi ai sistemi informativi
Dal punto di vista di raccomandazioni da fornire alle aziende sanitarie per quanto riguarda l'attività di monitoraggio consideriamo almeno due possibili strade:

- Appoggiarsi ad un fornitore esterno (nel caso in cui ci si appoggi ad un fornitore esterno per la gestione del proprio sistema informativo, sarà presumibilmente lo stesso soggetto), che offra adeguate garanzie sulla qualità e sicurezza del proprio servizio, ad esempio certificato (es. ISO/IEC 27001 e ISO27018). Attraverso l'adozione di questo servizio, il sistema informativo dell'azienda sanitaria dovrà risultare protetto da un efficiente sistema di difesa perimetrale basato su sistemi IPS/IDS,WAF (*web application firewall*), PAM (*privileged access management*) (DAM (*Database access management*) e con un valido servizio di SOC (*security operation center*), dotato di strumenti SIEM (*Security Information Event Management*) e con processi ben definiti di gestione degli allarmi e di incident management, per dare solo alcuni elementi. Il fornitore dovrà anche mantenere il proprio personale aggiornato in modo continuo sulle nuove minacce e vulnerabilità, e aggiornare corrispondentemente anche i propri strumenti di rilevazione.
- Implementare nella propria data farm un sistema centralizzato di tracciatura e di conseguenza definire un processo di monitoraggio che permetta di effettuare analisi e verifiche sui dati raccolti. Ovviamente entrano in gioco non solo aspetti di tipo tecnologico, ma soprattutto organizzativi e procedurali. L'azienda sanitaria dovrà infatti arrivare allo stesso livello di protezione e monitoraggio del caso precedente, ma attraverso risorse interne.

Il primo passo obbligatorio è la catalogazione delle informazioni che si intendono tracciare. Nei sistemi informativi, oggi siamo oberati da una molteplicità di informazioni di tracciatura di carattere "sistemistico" che dovrebbero essere monitorate, es. log di firewall, log di sistema del dominio log di sistema dei server, log di accesso alle applicazioni, log di sistema ed accesso al DB, log web server nel caso di esposizione di servizi su Internet per fare solo degli esempi, senza parlare degli audit log applicativi, quando necessari o richiesti da normativa, per un mantenimento/storicizzazione di quando o chi a modificato una particolare informazione, tenendo conto dei disposti normativi inerenti la conservazione documentale a norma.
Il secondo passo è la definizione dei tempi della conservazione che si vuole attuare che può variare a seconda della finalità richiesta, e che va considerata anche in relazione alla quantità di dati raccolti. In funzione di questi parametri deve essere definito anche il dimensionamento nel tempo delle aree di archiviazione.

Il terzo passo è l'implementazione di un sistema centralizzato di tracciatura. Perché centralizzato? Perché in tal modo e sicuramente più fattibile la conseguente esamina dei dati e l'eventuale realizzazione di procedure di correlazione degli eventi, ed inoltre perchè una gestione centralizzata ed effettuata con specifici criteri di sicurezza permette di evitare eventuali manipolazioni dei Log e quindi perdita o cancellazione di informazioni durante una condizione di attacco. Del resto le aziende sanitarie dovrebbero già aver implementato sistemi similari per la conservazione dei log di accesso delle figure di amministratori di sistema, in base al provvedimento del 2008 del garante Privacy, in merito. Anche in questo caso, come nei due precedenti, è necessario tener conto del valore legale dei documenti/record conservati.

Concentrandosi sui log di tipo sistemistico, una volta realizzate le procedure o i connettori per la centralizzazione delle informazioni sul SIEM casalingo, si apre il tema del monitoraggio e dell'analisi/correlazioni delle informazioni per l'identificazione di un eventuale accadimento fraudolento.

Difatti l'evidenza di una data breach può avvenire prevalentemente in tre modalità:

- Si viene avvertiti dall'autorità di polizia o dal CERT che i dati sono stati palesemente pubblicati o intercettati su server esterni alla rete dell'ente
- L'intrusione e/o il furto dei dati sono palesi (attacco che provoca crash del sistema, distruzione o cifratura del database (es cryptoloker) con relativa interruzione del servizio (in tal caso non è detto che il furto sia comunque avvenuto)
- Non vi è stato alcun evidente disservizio, ma analizzando i log si ha evidenza di una intrusione con tracce di totali o parziali "*exfiltration*" di dati

Mentre i primi due scenari sono evidenti, lo scenario tre (che può portare poi al caso 1)) è quello più complesso da esaminare, è dipendente dalla quantità di informazioni che ho a disposizione e dalla possibilità di effettuare delle correlazioni, e quindi di poter ricostruire tutto quanto accaduto.

E ovvio che l'azione di logging e di monitoraggio di conseguenza, richiedono da parte dell'azienda una organizzazione in termini di team di risorse e di strumenti da utilizzare non banale, e che comunque deve essere necessariamente implementata almeno per poter capire e comprendere, al fine di porre in atto delle *remediation* appropriate, per almeno evitare che il problema si amplifichi o si ripeta.

Di nuovo, il principale valore aggiunto del log e del monitoraggio (uso il termine automatizzato, poichè in questo caso non sarebbe umanamente possibile effettuarlo con persone) non dovrebbe essere solo quello di poter ricostruire un evento malevolo che è accaduto, ma principalmente ricorrendo a strumenti di detection automatizzati poter impedire, alle prime avvisaglie, l'effettuarsi di un attacco. Per fare un esempio pratico, se un'azienda sanitaria offre servizi di accesso ai propri applicativi su canale internet, non può assolutamente prescindere dall'uso di soluzioni di *web application firewall*, in grado di analizzare il contenuto del traffico su canale HTTP e HTTPS e poter di conseguenza tramite i meccanismi e gli algoritmi interni di verifica della sintassi utilizzata nelle URL poter riconoscere pattern di attacco e bloccarne l'esecuzione (dico bloccarne non loggare l'esecuzione volutamente). Questa modalità di individuazione e identificazione certa o in alcuni casi comunque sopra soglia e relativo blocco della chiamata/connessione, nel banale esempio citato, è la sola soluzione oggi percorribile poter ottenere une effettiva mitigazione del rischio informatico in tempo reale, anche con l'eventualità di effettuare il blocco di qualche falso positivo. Ogni altra azione delegata all'intervento umano non può che essere posteriore e unicamente di analisi decisionale sulla gestione delle policy.

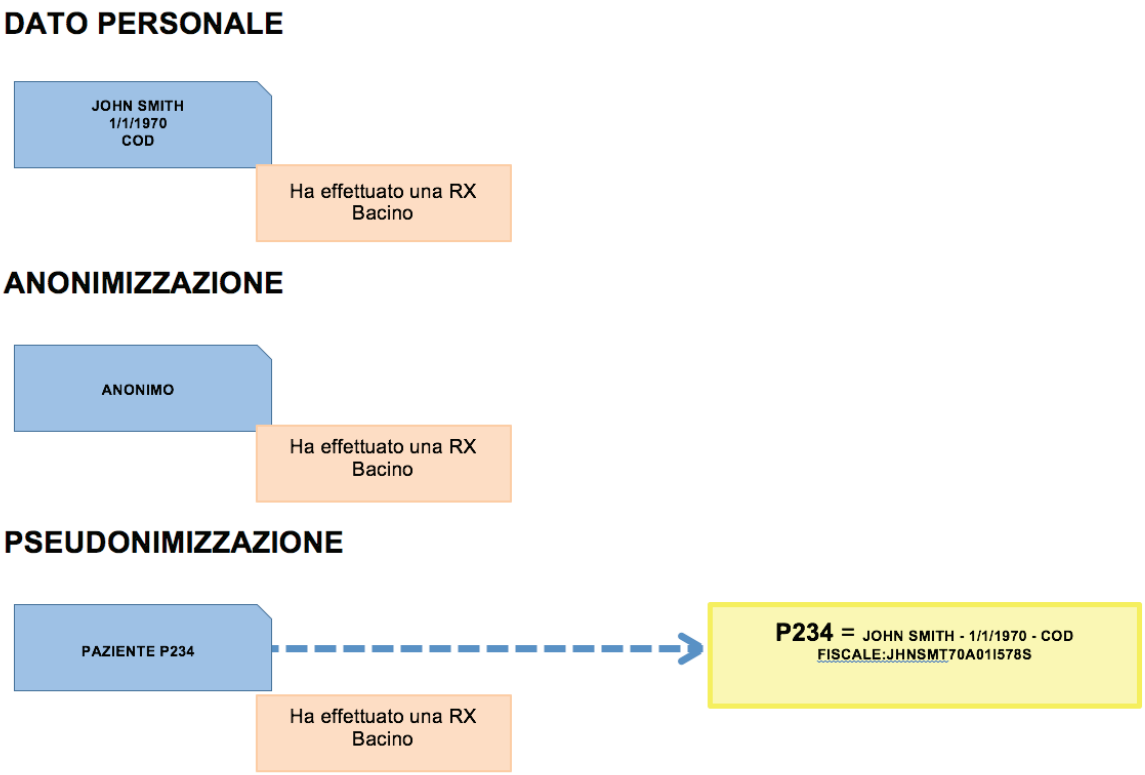
7.1 ——— Anonimizzazione e pseudonimizzazione

L'anonimizzazione e la pseudonimizzazione, ove non si padroneggi il significato di entrambi i termini, vengono spesso confusi e associati l'uno con l'altro. L'utilizzo di entrambe le tecniche si pone l'obiettivo di evitare l'identificazione del soggetto proprietario dei dati personali che vengono trattati.
Entrando nel dettaglio:

- per «pseudonimizzazione» si intende il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
- per «anonimizzazione» si intende il risultato del trattamento di dati personali allo scopo di impedire irreversibilmente l'identificazione della persona interessata (si vedano anche il documento del gruppo di lavoro WP29 sulle Tecniche di anonimizzazione del 10 aprile 2014)

In considerazione di quanto detto, la pseudonimizzazione non è un metodo di anonimizzazione, in quanto risulta essere reversibile, al contrario dell'anonimizzazione che rende i dati definitivamente non riconducibili all'identità del soggetto.

Per semplificare il concetto:



Considerando l'aspetto pratico di applicabilità di entrambe le tecniche possiamo analizzare nel dettaglio in cosa consistano.

Anonimizzazione

L'**anonimizzazione** è la tecnica con la quale si elimina la riconducibilità dei dati trattati alla persona identificata. Consiste quindi nell'eliminazione di tutti i dati identificativi o di qualsiasi mezzo che consenta di risalire ai dati originali e quindi al soggetto interessato.

Come recita il considerando 26 del GDPR, i principi di protezione dei dati non dovrebbero pertanto applicarsi a informazioni anonime, vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato.

Pseudominizzazione

La **pseudonimizzazione** è una tecnica che tenta di ridurre la correlabilità tra i dati trattati, o un insieme di essi, e la possibile identificazione del soggetto proprietario dei dati. Il GDPR cita spesso la pseudonimizzazione come tecnica di protezione dei dati. Si tratta infatti di una tecnica che è perfettamente in linea con le logiche di Privacy by Design. Infatti, è pratica comune utilizzare dati identificativi come indice, perché permettono una facile ed immediata riconducibilità all'interessato. Questa scelta rende più complesso intervenire sui dati identificativi. Viceversa, la logica di Privacy by Design ci richiede di fare in modo che i dati identificativi di default non siano disponibili, se non nei trattamenti per i quali siano strettamente necessari, utilizzando altri codici/indici per ricondurre i dati all'interessato. Questo tema è particolarmente critico nel contesto della Sanità, dove l'attenzione ad associare i dati all'interessato è ovviamente particolarmente alta.

I dati identificativi consentono di riconoscere facilmente una data persona. Per associare uno pseudonimo ai dati identificativi di una persona viene comunemente utilizzata una lista di corrispondenze. Finché tale lista è disponibile, la pseudonimizzazione è un processo reversibile.

La pseudonimizzazione, come anticipato precedentemente, risulta essere diversa dall'anonimizzazione, poiché trattasi di processo reversibile, purché questo sia possibile attraverso informazioni aggiuntive memorizzate separatamente dai dati pseudonimizzati.

Per esempio, per pseudonimizzare i dati del paziente JOHN SMITH, gli applicativi di gestione della refertazione o della cartella del paziente dovrebbero essere cosi organizzati:

- Si attribuisce alla scheda di JOHN SMITH un codice identificativo univoco;
- Si crea una tabella separata in cui quel codice è abbinato a tutte le informazioni che possono condurre all'identificazione per individuazione, correlazione o deduzione alla persona, come nome, email, numero di telefono, codice fiscale eccetera;
- Si eliminano dalla scheda dei dati pseudonimizzati i dati identificativi o pseudoidentificativi visti nel punto precedente, lasciando solo il codice identificativo come mezzo per ricollegare le due tabelle

Questo semplice esempio costituisce un'attuazione del GDPR che richiede che i dati personali, qualora sussistano rischi per i diritti e le libertà degli interessati, vengono archiviati in un formato che non consente l'identificazione diretta di un individuo senza utilizzare ulteriori informazioni, come le tabelle di mapping archiviate separatamente.

Ovunque si trovino queste informazioni sulle associazioni, queste devono essere archiviate separatamente e sottoposte a controlli che ne impediscano l'associazione a dati pseudonimizzati ai fini dell'identificazione. Il data masking e l'hashing sono alcuni esempi di tecnologie di pseudonimizzazione. Il data masking rappresenta una pratica standard per la pseudonimizzazione, utilizzata principalmente negli ambienti di dati "di non produzione" per lo sviluppo di software, di testing, di analisi. La pratica consiste nel sostituire i dati sensibili con dati fittizi, seppure realistici; Attraverso l'utilizzo del masking si tutela il valore dei dati per scopi di non produzione, eliminando il rischio di collegamento ai dati originali.
Il mascheramento dei dati può ovviamente essere applicato non solo ai dati nominativi, come nell'esempio sopra riportato, ma potrebbe essere applicato anche ai dati particolari (es sensibili). Già oggi molte patologie, o prestazioni sanitarie sono codificate tramite codici identificativi. Il problema è che tali codici rappresentano standard a livello nazionale e quindi de facto noti, di conseguenza non rendono applicabile il concetto di pseudonimizzazione.

Scelta della tecnica appropriata

La scelta di utilizzare l'anonimizzazione o la pseudonimizzazione va ponderata e valutata per ogni specifico trattamento in considerazione della specifica finalità e nel rispetto dei principi generali esposti nell'articolo 5 GDPR.
Il documento del gruppo di lavoro WP29 sulle Tecniche di anonimizzazione del 10 aprile 2014 espone in maniera esaustiva i pregi ed i difetti di ogni tecnica considerata e può essere utilizzato come guida per la scelta della tecnica più idonea al caso d'uso in oggetto.
A titolo esemplificativo si potrebbe scegliere tra:

a) Generalizzazione (l-diversità e k-anonimato) per le elaborazioni statistiche di aggregazione,
b) l'anonimizzazione tramite permutazione, preferibilmente in combinazione con l'aggiunta di rumore statistico per la predisposizione degli ambienti di sviluppo e test
c) la pseudonimizzazione tramite crittografia con chiave segreta per condividere dati tra differenti titolari per le sperimentazioni cliniche.

In ambito sanitario va tenuto in considerazione il debito informativo per finalità di rendicontazione e non solo nei confronti di Regione e Ministero che spesso preclude la possibilità di procedere all'anonimizzazione dei dati alla sorgente rendendo quasi obbligatoria la pseudonimizzazione.

Anche a supporto della pseudonimizzazione, è utile da una parte avere pochi repository di dati ai quali i diversi applicativi facciano riferimento, in modo da mantenere sotto controllo l'accesso a dati identificativi, e dall'altra, sempre in linea con le logiche di Privacy by Design, definire dei requisiti chiari per lo sviluppo, l'acquisizione e la manutenzione evolutiva degli applicativi e del middleware.

7.2 —— I diritti dell'interessato che impattano sulle applicazioni

La Struttura Sanitaria che tratti i dati degli interessati in formato elettronico deve assicurarsi che il sistema informatico adottato possa rispondere ai requisiti richiesti dal GDPR relativamente ai seguenti diritti dell'inte-

ressato (artt. 15- 20) con riferimento ai propri dati registrati nel sistema:

- Accesso
- Rettifica/integrazione/cancellazione
- Limitazione del trattamento
- Portabilità

Si premette che i dati devono essere conservati per il periodo stabilito dalla legge, che varia a seconda della tipologia dei dati (si va da "un anno" ad es. per i referti di laboratorio per i non ricoverati a "illimitato" ad es. per le cartelle cliniche) , pertanto i programmi applicativi devono essere in grado di gestire il periodo di data retention, fatta salvo il versamento in sistemi di conservazione a norma, in taluni casi obbligatorio.
I programmi applicativi utilizzati nella Struttura devono essere progettati e realizzati in modo tale che, a richiesta dell'interessato, si possa accedere agevolmente a tutti i dati riconducibili all'interessato stesso ("privacy by design") per effettuare una o più operazioni tra quelle sopra elencate.
Requisito fondamentale è una definizione attenta e articolata dei profili utenti e delle funzioni autorizzate per ciascun profilo, compresa quella di ricerca dei dati relativi all'interessato che si rivolge al Titolare per far valere i propri diritti.
Non meno importante è la presenza di una gestione centralizzata dei consensi : ogni dipartimentale deve raccogliere dall'interessato il consenso allo specifico trattamento dati, trasmettendo poi l'informazione a un software con funzioni di "consent manager" centrale che sia in grado di elaborare e distribuire le informazioni necessarie alla visualizzazione dei dati memorizzati, tenendo conto sia delle autorizzazioni dell'interessato che dei profili utenti che richiedono l'accesso ai dati.
Il processo di reperimento di tali dati sarà più rapido se la Struttura è in grado di gestire il Dossier Sanitario e se l'interessato ha dato il consenso al trattamento dei suoi dati tramite DS; in tal caso, la ricerca dei dati avverrà tramite l'identificativo univoco assegnatogli dal Sistema Informatico al primo accesso e utilizzato dai vari sottosistemi ("Dipartimentali") che trattano di volta in volta le prestazioni relative al paziente (referti diagnostici, cartelle cliniche di degenza, referti di pronto soccorso ecc.).
Se la Struttura non gestisce il Dossier Sanitario o se il paziente non ha dato il consenso alla gestione dei propri dati tramite DS, per il reperimento dei dati archiviati nel Sistema sarà necessario effettuare la ricerca dei dati nei vari Dipartimentali tramite cognome, nome e data di nascita dell'interessato o meglio tramite codice fiscale.
Una volta stabilita la metodologia adeguata per il reperimento dei dati archiviati nel Sistema Informatico, si potranno soddisfare le richieste dell'interessato sopra elencate.
In particolare, per quanto riguarda l'**accesso** si dovrà garantire la possibilità di tracciare, tramite specifici tools, l'elenco degli accessi ai dati effettuati: ciò presuppone ovviamente che ciascun utente del Sistema Informativo utilizzi proprie univoche credenziali, che i programmi registrino in apposito database ogni accesso effettuato ("log" degli accessi) e che sia possibile produrre tale elenco a richiesta dell'interessato.
A tale proposito sarebbe preferibile adottare nell'ambito del sistema informativo un protocollo standard come ad esempio "syslog" per la trasmissione a un sistema centrale dei "log" generati dalle varie applicazioni; esistono infatti sul mercato molteplici tools , alcuni anche free, in grado di elaborare i log memorizzati con tale protocollo, producendo output di varia utilità sia ai fini della sicurezza del sistema (ad esempio alert in caso di accessi non autorizzati a file, cartelle o applicazioni) sia ai fini del controllo degli accessi e delle

operazioni ad esempio di visualizzazione/modifica/cancellazione effettuate dagli utenti, compresi gli amministratori di sistema. Si ricorda che i log degli amministratori di sistema devono essere conservati in un apposito sistema normato dal CAD.
Per quanto riguarda **la rettifica/integrazione**, questa sarà possibile solo relativamente ai dati anagrafici dell'interessato ma non ai dati sanitari, per ovvi motivi legali ; tramite specifiche funzioni si dovrà garantire la possibilità di rettifica nell'archivio Anagrafe Centrale, ove presente, e/o nei Dipartimentali (diagnostica per immagini, laboratorio di analisi ecc.) dove, se i referti sono archiviati elettronicamente tramite firma digitale, si dovrà prevedere una gestione delle variazioni tramite identificazione di uno specifico processo stabilito (i.e. emissione di un nuovo referto firmato digitalmente a sostituzione del precedente, che comunque non verrà cancellato).
La rettifica dei dati dovrà essere comunicata anche agli eventuali operatori sanitari a cui eventualmente siano stati trasmessi; per tale motivo, è necessario che il software tenga traccia di tutti le operazioni di comunicazione dei dati verso terzi , effettuate ovviamente previa autorizzazione dell'interessato.

La **cancellazione** dei dati in una Struttura Sanitaria va trattata con particolare attenzione: non sarà ovviamente possibile per quanto riguarda le cartelle cliniche e i referti in quanto questi rappresentano un atto medico-legale che deve essere conservato a tutela degli operatori medici che hanno gestito tali dati. Sarà invece possibile , su richiesta dell'interessato , escludere tutti i referti e/o le cartelle cliniche o solo alcuni di essi, dal trattamento tramite Dossier Sanitario : in tal caso i dati resteranno archiviati per la consultazione, per il tempo di legge previsto, da parte dei professionisti sanitari che li hanno redatti, e per questioni di contenzioso legale mentre saranno "oscurati" a tutti gli altri operatori sanitari che accedono al Sistema.
Sarà inoltre sempre possibile richiedere la cancellazione dei dati registrati al fine di una profilazione dell'interessato, raccolti e conservati sempre previo suo consenso esplicito.

La **limitazione** del trattamento potrebbe essere richiesta dall'interessato ad esempio quando, trascorsi i tempi consentiti di conservazione di un referto, la Struttura si appresti a cancellarlo ma l'interessato abbia necessità di conservarlo a fini legali (ad es. per l'esercizio o la difesa di un diritto in sede giudiziaria) : in tal caso il Sistema Informativo deve essere in grado di rendere indisponibile il referto agli utenti autorizzati, oscurando quindi il riferimento e il contenuto del referto stesso, limitando l'accesso al Titolare del trattamento e/o a persona da egli espressamente delegata; ciò implica la definizione di un profilo "super user" e delle funzioni consentite questo profilo.

Allegato 1

Format di una possibile scheda di un'attività di trattamento contenuta nel registro

NOME TRATTAMENTO	
ID TRATTAMENTO	

A. DATI DI CONTATTO

Titolare		Rappresentante del Titolare		Contitolari		Responsabile Protezione Dati	
Struttura	**Contatti**	**Struttura**	**Contatti**	**Struttura**	**Contatti**	**Struttura**	**Contatti**

B. FINALITÀ DEL TRATTAMENTO

Informativa		Tipologia di consenso	
Ref.	**Descrizione**	**Ref.**	**Descrizione**

C. CATEGORIE DI INTERESSATI E DI DATI TRATTATI

Categorie di Interessati del Trattamento				Natura del dato trattato
☐ Pazienti	☐ Dipendenti	☐ Candidati	☐ Fornitori	☐ Personale comune
☐ Prospect	☐ Collaboratori	☐ Familiari	☐ Soggetti terzi	☐ Sensibile
				☐ Giudiziario

Categoria del dato trattato e soggetti interessati dal trattamento

Categoria del dato	Pazienti	Prospect	Dipendenti	Collaboratori	Candidati	Familiari	Fornitori	Soggetti terzi
☐ Dati identificativi	☐	☐	☐	☐	☐	☐	☐	☐
☐ Dati comportamentali	☐	☐	☐	☐	☐	☐	☐	☐
☐ Dati sensibili	☐	☐	☐	☐	☐	☐	☐	☐
☐ Dati genetici	☐	☐	☐	☐	☐	☐	☐	☐
☐ Dati giudiziari	☐	☐	☐	☐	☐	☐	☐	☐
☐ Dati relativi alla gestione del rapporto di lavoro	☐	☐	☐	☐	☐	☐	☐	☐
☐ Cookies	☐	☐	☐	☐	☐	☐	☐	☐
☐ Log di sistema (Utenti e AdS)	☐	☐	☐	☐	☐	☐	☐	☐

D. CATEGORIE DI DESTINATARI UE e EXTRA UE

Nome	Finalità del trasferimento	Tipologia di destinatario	UE	Extra UE	Garanzie adeguate in caso di destinatari extra UE)					
					Consenso	Privacy Shield (USA)	BCR	Data Protection Agreement	Model contract clauses	Certificazioni
		☐ Titolari ☐ Resp. esterni ☐ Org. internaz.	☐	☐	☐	☐	☐	☐	☐	☐
		☐ Titolari ☐ Resp. esterni ☐ Org. internaz.	☐	☐	☐	☐	☐	☐	☐	☐
		☐ Titolari ☐ Resp. esterni ☐ Org. internaz.	☐	☐	☐	☐	☐	☐	☐	☐

E. CONSERVAZIONE E CANCELLAZIONE DEI DATI

Categoria del dato trattato	Periodo di conservazione	Action al termine del periodo di retention	
		Anonimizzazione	Cancellazione
☐ Dati identificativi		☐	☐
☐ Dati comportamentali		☐	☐
☐ Dati sensibili		☐	☐
☐ Dati genetici		☐	☐
☐ Dati giudiziari		☐	☐
☐ Dati relativi alla gestione del rapporto di lavoro		☐	☐
☐ Cookies		☐	☐
☐ Log di sistema (Utenti e AdS)		☐	☐

F. STRUMENTI UTILIZZATI PER IL TRATTAMENTO

ID	Nome	Descrizione e utilizzo	Note

G. MISURE DI SICUREZZA ORGANIZZATIVE*

Distribuzione dei Ruoli e Responsabilità	**Formazione**	**Policy, Procedure, Istruzioni operative**
Meccanismi incentivanti per i soggetti coinvolti	**Misure per Privacy by Design / Privacy by Default**	**Clausole contrattuali / SLA con le terze parti interessate**
Misure prescrittive organizzative per amministratori di sistema	**Misure prescrittive organizzative per l'utilizzo delle risorse informatiche**	**Misure prescrittive organizzative per videosorveglianza**
Misure prescrittive organizzative per FSE/CE	**Misure prescrittive organizzative per i trial clinici**	**Misure prescrittive organizzative per la refertazione on-line**
Misure prescrittive organizzative per dati genetici	**Misure prescrittive organizzative per marketing su dati sanitari**	**Monitoraggio periodico delle misure organizzative e operative**

H. PROFILO DI RISCHIO

Profilo di rischio preliminare	**Inserire data** Inserire livello di rischio (Non Alto/Alto)	**Valutazione preliminare Autorità Garante (solo per trattamenti con profilo di rischio residuo Alto dopo DPIA)**	**Inserire data** Esiti della consultazione preventiva
Profilo di rischio post Data Protection Impact Assessment	**Inserire data** Inserire livello di rischio (Non Alto/Alto)		Link al provvedimento

* Le misure di sicurezza tecniche sono associate ai singoli strumenti di trattamento, nelle relative schede (e.g. Pseudonimizzazione e cifratura dei dati)

Allegato 2

Un possibile elenco di attività di trattamento desunta dagli attuali regolamenti regionali emanati ai sensi degli artt. 20 e 21 del Codice Privacy in conformità agli schemi tipo approvati dall'Autorità Garante Privacy *Lista esemplificativa dei trattamenti di dati sensibili nell'ambito di aziende sanitarie*

Nomine e designazioni da parte delle Aziende sanitarie

Instaurazione e gestione del rapporto di lavoro del personale inserito a vario titolo, compreso il collocamento obbligatorio e assicurazioni integrative

Attività sanzionatoria e di tutela amministrativa e giudiziaria

Attività correlata alla mediazione obbligatoria finalizzata alla conciliazione delle controversie civili e commerciali

Attività amministrative correlate all'anagrafe patrimoniale dei titolari di cariche elettive, di cariche direttive e di incarichi dirigenziali

Assicurazione per i dipendenti da infortunio o infermità, sui rischi di morte, invalidità permanente o temporanea, e assicurazione invalidità permanente o temporanea e assicurazione invalidità

Gestione dei dati relativi ai partecipanti a corsi ed attività formative

Videosorveglianza

Gestione dei fornitori

Tutela dei rischi infortunistici e sanitari connessi con gli ambienti di vita e di lavoro

Sorveglianza epidemiologica delle malattie infettive e diffusive e delle tossinfezioni alimentari

Attività amministrative e certificatorie correlate alle vaccinazioni e alla verifica assolvimento obbligo vaccinale

Attività amministrative correlate ai programmi di diagnosi precoce

Attività fisica e sportiva

Attività di assistenza socio-sanitaria a favore di fasce deboli di popolazione e di soggetti in regime di detenzione

Medicina di base - pediatria di libera scelta - continuità assistenziale (guardia medica notturna e festiva, guardia turistica)

"Assistenza sanitaria di base: riconoscimento del diritto all'esenzione per patologia/invalidità e gestione archivio esenti"

Assistenza sanitaria di base: assistenza sanitaria in forma indiretta

Cure all'estero urgenti e programmate

Assistenza sanitaria di base: assistenza agli stranieri in Italia (particolari categorie)

Assistenza integrativa

Assistenza protesica

Assistenza domiciliare programmata e integrata

"Attività amministrative correlate all'assistenza a soggetti non autosufficienti, a persone con disabilità fisica, psichica e sensoriale e a malati terminali nei regimi residenziale, semiresidenziale ambulatoriale (ex art. 26 della L. 833/1978) e domiciliare"

Assistenza termale

"Attività amministrativa, programmatoria, gestionale e di valutazione relativa all'assistenza ospedaliera in regime di ricovero"

"Attività amministrativa, programmatoria, gestionale e di valutazione concernente l'attività immuno-trasfusionale"

"Attività amministrativa, programmatoria gestionale e di valutazione concernente la donazione, il trapianto di organi, tessuti e cellule"

Soccorso sanitario di emergenza/urgenza sistema "118". Assistenza sanitaria di emergenza

Attività amministrative correlate ad assistenza specialistica, ambulatoriale e riabilitazione

Promozione e tutela della salute mentale

Attività amministrative correlate alle dipendenze (tossicodipendenze e alcooldipendenze)

Assistenza socio-sanitaria per la tutela della salute materno-infantile ed esiti della gravidanza

Attività amministrative correlate all'assistenza farmaceutica territoriale e ospedaliera

Sperimentazione clinica

Farmacovigilanza e rilevazione reazioni avverse a vaccini e farmaci

Attività amministrative correlate all'erogazione a totale carico del servizio sanitario nazionale, qualora non vi sia alternativa terapeutica valida, di medicinali inseriti in apposito elenco predisposto dall'Agenzia Italiana del Farmaco

Attività amministrative correlate all'assistenza a favore delle categorie protette (morbo di Hansen)

"Attività amministrativa programmatoria, gestionale e di valutazione concernente l'assistenza ai nefropatici cronici in trattamento dialitico"

"Attività medico-legale inerente l'istruttoria delle richieste di indennizzo per danni da vaccinazioni obbligatorie, trasfusioni e somministrazione di emoderivati"

"Attività medico-legale inerente gli accertamenti finalizzati al sostegno delle persone con disabilità (riconoscimento dello stato di invalidità, cecità e sordità civili, della condizione di handicap ai sensi della L. 104/92, accertamenti per il collocamento mirato al lavoro delle persone con disabilità ai sensi della L. 68/99)"

"Attività medico-legale inerente l'accertamento dell'idoneità in ambito di diritto al lavoro (assunzione nel pubblico impiego: idoneità allo svolgimento di attività lavorative; controllo dello stato di malattia dei dipendenti pubblici e privati; accertamenti sanitari di assenza di tossicodipendenza o di assunzione di sostanze

stupefacenti o psicotrope in lavoratori addetti a mansioni che comportino particolari rischi per la sicurezza, l'incolumità e la salute di terzi)"

"Attività medico-legale inerente l'accertamento dell'idoneità al porto d'armi, ai fini della sicurezza sociale"

"Attività medico-legale inerente l'accertamento dell'idoneità alla guida, ai fini della sicurezza sociale"

Consulenze e pareri medico-legali in tema di riconoscimento della dipendenza delle infermità da causa di servizio

Consulenze e pareri medico-legali in tema di ipotesi di responsabilità professionale sanitaria, di supporto all'attività di gestione del rischio clinico, informazione e consenso ai trattamenti sanitari e consulenze e pareri in materia di bioetica

Attività medico-legale in ambito necroscopico

Attività di programmazione, gestione, controllo e valutazione dell'assistenza sanitaria

Attività amministrative correlate alla gestione e verifica sull'attività delegata a soggetti accreditati o convenzionati del SSN

Allegato 3

Modello di DPA

Data Processing Agreement

Parti

Il presente accordo è concluso tra le parti [********] da ora in avanti anche Titolare e [**********] da ora in avanti anche Responsabile.

Premessa

Tramite il presente Data Processing Agreement le parti intendono regolare il proprio rapporto in relazione alle attività di trattamento di dati personali con particolare attenzione alla protezione dei dati.

Gli allegati formano parte integrante del presente Data Processing Agreeement.

Definizioni

1. La terminologia del Data Processing Agreement si rifà a quanto definito dal Regolamento UE 679/2016, per quanto non definito dal regolamento si forniscono le seguenti definizioni:

«Regolamento»: REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);

«Titolare o Titolare del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro orga-

nismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali;

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

«Subresponsabile o Subresponsabile del Trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto di un Responsabile o Subresponsabile;

«Incaricati o Incaricati del trattamento»: le persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare o dal responsabile;

«Accordo»: il presente Data Processing Agreement;

Obblighi del Responsabile

Principi generali da osservare

Il Responsabile si impegna a trattare i dati in ottemperanza ai principi sanciti:

dall'ordinamento nazionale ed europeo in materia di protezione dei dati;

dall'articolo 5 del Regolamento;

Obblighi generali del Responsabile

Il Responsabile è in possesso di competenze, formazione, capacità ed affidabilità idonee a mettere in atto misure tecniche e organizzative affinché i trattamenti svolti sotto la sua responsabilità soddisfino i requisiti della normativa di settore, con particolare attenzione alla tutela dei diritti e libertà dell'interessato.

Il Responsabile utilizza i dati personali oggetto del trattamento solo per le finalità indicate nell'Allegato A "Attività di trattamento", in nessun caso potrà utilizzare i dati per fini propri.

Il Responsabile tratta i dati d'accordo con le istruzioni impartite dal Titolare.

Rendicontazione, audit e collaborazione

Se il Responsabile del trattamento ritiene che alcune delle istruzioni violino una qualsiasi disposizione di legge comunitaria o nazionale lo comunica al Titolare senza ingiustificato ritardo.

Il Responsabile mette a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente atto, consente e contribuisce alle attività di revisione, comprese le ispezioni, realizzate dal Titolare o da un altro soggetto da questi incaricato.

Tenuta del registro delle attività di trattamento

Il Responsabile si impegna a redarre per iscritto un registro delle attività di trattamento effettuate per conto del Titolare, che contenga almeno le seguenti informazioni:

nome e i dati di contatto del Responsabile o dei Responsabili del trattamento, di ogni Titolare del trattamento per conto del quale il Responsabile agisce, del rappresentante del Titolare del trattamento o del Responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;

categorie delle attività di trattamento effettuate per conto di ogni Titolare del trattamento;

ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, com-

presa l'identificazione del paese terzo o dell'organizzazione internazionale corredata dalla documentazione che legittima tale trasferimento;

una descrizione generale delle misure di sicurezza tecniche e organizzative adottate;

Comunicazione a terzi

Il Responsabile non comunica i dati a terzi a meno che non sia espressamente autorizzato a farlo dal Titolare.

Il Responsabile può trasmettere dati ad altri Responsabili per conto dello stesso Titolare, in conformità con le istruzioni da questo fornite. In questo caso, il Titolate identificherà, in anticipo e per iscritto, il soggetto a cui vanno comunicati i dati, i dati da comunicare e le misure di sicurezza da applicare alla comunicazione.

Se il responsabile intende trasferire tutti o alcuni dati personali oggetto dell'Accordo verso un paese terzo o un'organizzazione internazionale, si impegna ad informare il Titolare prima di procedere al trasferimento, fornendo indicazioni sulla base legale che legittima il trasferimento.

Ricorso ad altri Responsabili e Subresponsabili [Una delle seguenti opzioni]

Il responsabile non può ricorre o nominare ad altro responsabile, senza previa espressa e scritta autorizzazione del Titolare.

Il responsabile è autorizzato a nominare altro responsabile per lo svolgimento delle attività di trattamento dei dati elencate nell'Allegato A "Attività di trattamento" e contrassegnate come tali.

Il responsabile è autorizzato a nominare altro responsabile previa notifica al Titolare salvo suo diritto di opposizione.

Requisiti minimi da imporre ad altri Responsabili e Subresponsabili

Qualora il Responsabile nomini altro Responsabile del trattamento su tale altro responsabile del trattamento sono imposti mediante atto scritto, gli stessi obblighi in materia di protezione dei dati contenuti nel presente atto.

Qualora il Responsabile nomini altro Responsabile del trattamento e quest'ultimo ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile iniziale conserva nei confronti del Titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile.

Riservatezza dei dati trattati

Il Responsabile si impegna a mantenere la segretezza e riservatezza riguardo a dati e informazioni personali e non ai quali abbia avuto accesso in virtù del presente incarico anche dopo il termine del presente incarico.

Il Responsabile garantisce che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;

Incaricati del trattamento

Il Responsabile si impegna a:

individuare tra i propri collaboratori, quelli che compiono operazioni di trattamento dati personali e nominarli Incaricati del trattamento;

recepire le istruzioni impartite da Titolari e Responsabili, comunicandole agli Incaricati del trattamento;

adoperarsi al fine di rendere effettive le suddette istruzioni, curando in particolare il profilo della riservatezza, della sicurezza di accesso e dell'integrità dei dati;

stabilire le modalità di accesso ai dati e l'organizzazione del lavoro degli Incaricati, avendo cura di adottare preventivamente misure organizzative adeguate al rischio per diritti e libertà delle persona fisiche.

Diritti dell'interessato [possibilità di richiedere al responsabile di dare seguito a richieste interessati in autonomia]

Il Responsabile assiste il Titolare adottando misure tecniche e organizzative adeguate atte a dare seguito alle richieste di esercizio dei diritti da parte degli interessati di cui al capo III del Regolamento tra le altre:

Diritti di accesso, rettifica, cancellazione e opposizione;

Diritto alla limitazione del trattamento;

Diritto alla portabilità dei dati;

Diritto di opposizione ad un processo decisionale automatizzato relativo alle persone fisiche;

Violazione dei dati personali

In caso di violazione, fuga o perdita di dati personali, il responsabile del trattamento informa il Titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

Nell'informare il Titolare il Responsabile comunica le seguenti informazioni:

descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati coinvolti, nonché le categorie e il numero approssimativo di dati personali oggetto della violazione;

comunica il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere ulteriori informazioni;

descrivere le misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi sui diritti e libertà delle persone fisiche;

descrivere le probabili conseguenze della violazione dei dati personali;

Valutazione d'impatto

Se si rende necessaria una Valutazione d'impatto sulla protezione dei dati, in merito alle attività di trattamento oggetto del presente Accordo, il Responsabile assiste il Titolare nella redazione della Valutazione d'impatto sulla protezione dei dati;

Consultazione preventiva

Se si rende necessaria la Consultazione preventiva dell'autorità di controllo, in merito alle attività di trattamento oggetto del presente accordo, il Responsabile assiste il Titolare fornendogli tutte le informazioni necessarie per la Redazione della Consultazione preventiva;

Responsabile della Protezione dei Dati

Quando necessario sulla base delle norme nazionali ed europee, il Responsabile designa un Responsabile

della protezione dei dati.

Misure di sicurezza

Tenendo conto della natura, dell'oggetto, del contesto e delle finalità del trattamento, ma anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il Responsabile del trattamento mette in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio.

Il responsabile deve implementare misure che garantiscano:

la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi in uso ai fini dello svolgimento delle Attività di trattamento;

la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico;

la verifica e valutazione periodica dell'efficacia delle misure tecniche e organizzative;

Nello specifico il Responsabile deve garantire l'implementazione delle seguenti misure di sicurezza indicate nell'Allegato B "Misure di sicurezza".

Termine del rapporto [una delle due o entrambe le opzioni]

Al termine della prestazione dei servizi che comportano l'attività di trattamento, il Responsabile dovrà:

restituire i dati personali al Titolare del Trattamento ed eliminarli dalla propria infrastruttura informatica ed archivi cartacei, fornendo al Titolare idonea dichiarazione scritta dell'avvenuta distruzione dei dati.

eliminarli in maniera permanente dalla propria infrastruttura informatica ed archivi cartacei, fornendo al Titolare idonea dichiarazione scritta dell'avvenuta distruzione dei dati.

Obblighi del Titolare

Il Titolare fornisce istruzioni precise al Responsabile sulle modalità di trattamento dei dati (allegato C), sulle categorie di dati e sulla finalità per le quali vengono trattati.

Il Titolare garantisce che i dati siano stati raccolti in maniera lecita, per finalità determinate, (indicate nell'allegato A), e che i dati siano adeguati, pertinenti e limitati a quanto necessario per il perseguimento delle finalità per cui sono raccolti.

Responsabilità

Se il Responsabile del trattamento viola una delle disposizioni dell'Accordo determinando le finalità e i mezzi del trattamento, è considerato Titolare delle attività di trattamento per le quali ha determinato in autonomia finalità e mezzi del trattamento.

Il Responsabile risponde per il danno causato dal trattamento in solido con il Titolare, il quale si potrà rifare sul Responsabile nel caso questo o un Subresponsabile non abbia adempiuto gli obblighi del presente atto o abbia agito in modo difforme o contrario rispetto alle legittime istruzioni del Titolare del trattamento.

Allegati

Allegato A: "Attività di trattamento"

Allegato B: "Misure di sicurezza"

Allegato C: "Istruzioni su mezzi e modalità trattamento"

Allegato 4

IL TRASFERIMENTO DEI DATI VERSO PAESI TERZI

Il trasferimento di dati fuori dal territorio comunitario è una situazione, oggi molto più frequente di quanto non si pensi.

Solo a titolo di esempio molti dei soggetti che utilizzano servizi online, servizi cloud based, servizi di accesso remoto ecc. trasferiscono i dati fuori dalla UE, in quanto li caricano su server o cloud collocati fuori dl territorio UE.

Occorre pertanto prestare attenzione per verificare che questo trasferimento sia conforme al nuovo Regolamento.

Il Regolamento - come già prima la Direttiva 95/43/CEE - stabilisce che un soggetto (es. titolare o responsabile) può effettuare un trasferimento di dati verso paesi terzi solo in presenza di alcune condizioni:

- trasferimento sulla base di una decisione di adeguatezza (art. 45 del Regolamento)
- trasferimento soggetto a garanzie adeguate (art. 46 del Regolamento)
- trasferimento in forza di norme vincolanti d'impresa (art. 47)
- trasferimento in presenza di specifiche situazioni (art. 49)

Sotto una analisi più dettagliata della casistica

28. NB Per un errore di traduzione il testo dell'art. 40, comma 2, lett. b) del Regolamento 2016/679 nella versione italiana indica il termine "responsabile" anziché il termine "Titolari".

trasferimento sulla base di una decisione di adeguatezza (art. 45 del Regolamento)	
Disciplina	Commento
Art. 45 Il trasferimento di dati verso il destinatario di un paese terzo può aver luogo se la UE riconosce che tale paese presenta garanzia di tutela adeguate: si tratta della c.d Decisioni di Adeguatezza I fattori che possono influenzare una decisione sull'adeguatezza includono, tra l'altro: □ lo stato di diritto e protezioni legali per i diritti umani e le libertà fondamentali; □ l'accesso ai dati trasferiti da parte delle autorità pubbliche; □ esistenza e l'effettivo funzionamento di una autorità di protezione dei dati ; □ impegni internazionali e obblighi in materia di protezione dei dati personali . La Commissione può dichiarare i paesi terzi (o di un territorio, un settore specifico, o di un'organizzazione internazionale) per essere Giurisdizioni adeguata.	L'attuale elenco della Decisioni di adeguatezza può essere controllato qui http://www.garanteprivacy.it/home/provvedimenti-normativa/normativa/normativa-comunitaria-e-intenazionale/trasferimento-dei-dati-verso-paesi-terzi#1 Come noto in seguito alla decisione della Corte di Giustizia 6 ottobre 2015 - caso di Schrems l'accordo di adeguatezza Safe Harbor USA-UE non è stato ritenuto idoneo a salvaguardare le situazioni giuridiche dei cittadini europei. Il Safe Harbour è stato oggi sostituito dall'accordo UE-USA denominato Privacy Shield.
Art.45 comma 3 e -5) Considerando 93 (2) - (3) Le decisioni di adeguatezza sono soggette ad una revisione periodica, almeno ogni quattro anni, tenendo conto di tutti gli sviluppi rilevanti. La Commissione può revocare, modificare o sospendere le decisioni di adeguatezza nei confronti di quegli stati che non garantiscano un adeguato livello di protezione dei dati.	Come illustrato nella sentenza Schrems le decisioni di adeguatezza possono riviste in ragione del fatto che gli ordinamenti statali possono cambiare e quindi può verificare una condizione per cui il livello di protezione può cambiare. Le decisioni di adeguatezza adottate nell'ambito del GDPR rimangono valide per un massimo di 4 anni e possono essere modificate, sospese o abrogate. Questo può incidere sull'affidamento che le società possono fare sulle decisioni stesse.

Nell'ipotesi in cui non vi sia una una Decisione di Adeguatezza tra la UE e lo stato ove i dati vengono trasferiti, si dovrò optare i successivi strumenti giuridici.

trasferimento soggetto a garanzie adeguate (art. 46 del Regolamento)	
Casi di trasferimento SENZA autorizzazione dell'autorità di controllo Possono essere effettuati trasferimenti senza autorizzazione ove sussista uno dei seguenti elementi:	
a) uno strumento giuridicamente vincolante e avente efficacia esecutiva tra autorità pubbliche o organismi pubblici	Nel settore pubblico il trasferimento in un paese terzo può avvenire senza la necessità di un'autorizzazione specifica dell'autorità di controllo I soggetti che operano in alcuni settori (es ricerca) possono beneficiare della capacità delle autorità pubbliche nazionali per trasferire legalmente dati tra di loro in forza dell'esistenza di tali strumenti
b) norme vincolanti d'impresa in conformità dell'articolo 47;	La disciplina di tali norme è poi meglio approfondita all'art. 47
c) clausole tipo di protezione dei dati adottate dalla Commissione secondo la procedura d'esame di cui all'articolo 93, paragrafo 2;	Si tratta di clausole tipo (standard model clause) adottate dalla Commissione Si tratta di clausole allegate ai contratti di servizio o agli intercompany agreement Le clausole in vigore sono scaricabili qui http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm
d) clausole tipo di protezione dei dati adottate da un'autorità di controllo e approvate dalla Commissione secondo la procedura d'esame di cui all'articolo 93, paragrafo 2;	Si tratta di una novità introdotta del Regolamento Sono clausole analoghe a quelle di cui sopra che devono comunque essere approvate dalla commissione .
e) un codice di condotta approvato a norma dell'articolo 40,unitamente all'impegno vincolante ed esecutivo da parte del titolare del trattamento o del responsabile del trattamento nel paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli interessati;	Si tratta dei codici di condotta analizzati nell'apposito capitolo Oltre al rispetto del codice di condotta occorre poi che i soggetti abbiano stipulato tra loro un contratto che li obbliga al rispetto del codice stesso

f) un meccanismo di certificazione approvato a norma dell'articolo 42, unitamente all'impegno vincolante ed esigibile da parte del titolare del trattamento o del responsabile del trattamento nel paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli interessati.	Stesse considerazioni di cui sopra
Casi di trasferimento **CON autorizzazione dell'autorità di controllo** Possono essere effettuati trasferimenti CON l'autorizzazione dell'Autorità competente ove sussista uno dei seguenti elementi:	
a) clausole contrattuali intervenute tra il titolare del trattamento o il responsabile del trattamento e il titolare del trattamento, il responsabile del trattamento o il destinatario dei dati personali nel paese terzo o nell'organizzazione internazionale;	si tratta dell'ipotesi in cui i soggetti (titolare e responsabile) stipulino un contratto ad hoc di natura private per disciplinare il trasferimento di dati in questo caso tali clausole dovranno essere approvata espressamente dall'Autorità di controllo
b) disposizioni da inserire in accordi amministrativi tra autorità pubbliche o organismi pubblici che comprendono diritti effettivi e azionabili per gli interessati.	Si tratta della stessa ipotesi di cui sopra, tranne che il contratto interviene tra due pubbliche amministrazioni

all'interno di una impresa poi di potranno applicare anche le c.d. norme vincolanti d'impresa

trasferimento in forza di norme vincolanti d'impresa (art. 47)	
Le norme vincolanti di impresa devono essere APPROVATE dall'autorità competente l'approvazione da parte dell'Autorità avviene in presenza dei seguenti requisiti:	
Le norme vincolanti di impresa devono essere giuridicamente vincolanti e devono applicarsi a tutti i membri interessati del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune, compresi i loro dipendenti;	Anche in qusto caso si tratta di uno strumento di natura contrattuale La ratio della norma sta nel fatto che trattandosi di trasferimenti continuativi tra soggetti dello stesso gruppo, la decisione di farsi approvare norme vincolanti d'impresa (Binding Corporate Rules - BCR) consente di poter trasferire i dati in maniera pià agevole Le norme devono trovare applicazione per tutte le società del gruppo
Le norme di impresa devono conferire espressamente agli interessati diritti azionabili in relazione al trattamento dei loro dati personali;	Si tratta ovviamente di una tutela per gli interessati
Le norme vincolanti di impresa soddisfino i requisiti di cui al paragrafo 2.	Le BCR possono essere apporovate dall'Autorità Competente solo se forniscono idenee garanzie di tutela (adeguatezza) elencate nel paragrafo n. 2 dello stesso articolo

In tutti i casi diversi da quelli sopra, si potranno trasferire i dati solo ove sussistano le seguenti specifiche situazioni

trasferimento in presenza di specifiche situazioni (art. 49)	
Si applica solo nei casi in cui non vi sia una decisione di adeguatezza e non vi siano garanzia adeguate Le specifiche situazioni possono essere	
a) l'interessato abbia esplicitamente acconsentito al trasferimento proposto, dopo essere stato informato dei possibili rischi di siffatti trasferimenti per l'interessato, dovuti alla mancanza di una decisione di adeguatezza e di garanzie adeguate;	Si tratta del consenso informato dell'interessato. Si precisa che l'interessato deve essere informato degli specifici rischi connessi al trasferimento
b) il trasferimento sia necessario all'esecuzione di un contratto concluso tra l'interessato e il titolare del trattamento ovvero all'esecuzione di misure precontrattuali adottate su istanza dell'interessato;	si deve trattare di casi eccezionali e dettati da effettive "necessità". il WP 29 nel "*Working document on a common interpreta tion of Article 26(1) of Directive 95/46/EC of 24 October 1995 (on 25 November 2005)*" circa la nozione di "necessità" stabilisce che vi deve essere "uno stretto legame tra la persona interessata e le finalità del contratto"
c) il trasferimento sia necessario per la conclusione o l'esecuzione di un contratto stipulato tra il titolare del trattamento ed un'altra persona fisica o giuridica a favore dell'interessato;	si veriifca la condizione quando il trasferimento è necessario per conlcudere o eseguire un contratto stipulato tra il titolare del trattamento ed un'altra persona fisica o giuridica, purchè il contratto sia a favore dell'intereressato
d) il trasferimento sia necessario per importanti motivi di interesse pubblico;	si tatta dei casi elencati nel considerando 112 □ scambio internazionale di dati tra autorità garanti della concorrenza, □ amministrazioni fiscali o doganali, autorità di controllo finanziario, servizi competenti in materia di sicurezza □ sociale o sanità pubblica, ad esempio in caso di ricerca di contatti per malattie contagiose o al fine di ridurre e/o □ eliminare il doping nello sport

e) il trasferimento sia necessario per accertare, esercitare o difendere un diritto in sede giudiziaria;	questo caso comprende anche l'accertamento o la difesa del diritto stesso anche nelle fasi propedeutiche all'instaurazione del giudizio
f) il trasferimento sia necessario per tutelare gli interessi vitali dell'interessato o di altre persone, qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;	si tratta dei casi in cui vi è incapacità del soggetto a rilasciare il consenso e contemporaneamente sussiste un intersse vitale del soggetto stesso
g) il trasferimento sia effettuato a partire da un registro che, a norma del diritto dell'Unione o degli Stati membri, mira a fornire informazioni al pubblico e può esser consultato tanto dal pubblico in generale quanto da chiunque sia in grado di dimostrare un legittimo interesse, solo a condizione che sussistano i requisiti per la consultazione previsti dal diritto dell'Unione o degli Stati membri.	Circa tale tipologia di trasferimento il Considerano 111 precisa chein questo caso il trasferimento non dovrebbe riguardare la totalità dei dati personali o delle categorie di dati contenuti nel registro; inoltre, quando il registro è destinato a essere consultato dalle persone aventi un legittimo interesse, i dati possono essere trasferiti soltanto se tali persone lo richiedono o ne sono destinatarie, tenendo pienamente conto degli interessi e dei diritti fondamentali dell'interessato

Allegato 5

I CODICI DI CONDOTTA E I MECCANISMI DI CERTIFICAZIONE

Il Regolamento prevede quale novità la possibilità per il Titolare ed il Responsabile di aderire a dei codici di condotta e/o a meccanismi di certificazione quale elemento per dimostrare la conformità alle disposizioni del Regolamento.

I CODICI DI CONDOTTA

I **codici di condotta**, disciplinati dagli artt. 40 e 41 del Regolamento, possono essere **elaborati**, così come **modificati o prorogati**, dalle associazioni e dagli altri organismi rappresentanti le categorie di Titolari o Responsabili del trattamento con il fine di **precisare l'applicazione del Regolamento** ad esempio con riferimento ai seguenti **aspetti**:

il **trattamento corretto e trasparente** dei dati;

i **legittimi interessi** perseguiti dai Titolari[28] del trattamento in contesti specifici;

la **raccolta** dei dati personali;

la **pseudonimizzazione** dei dati personali;

l'**informazione** fornita al pubblico e agli interessati;

l'**esercizio dei diritti** degli interessati;

l'**informazione fornita e la protezione dei minori** e le modalità con cui è ottenuto il consenso dei titolari della responsabilità genitoriale sul minore;

le **misure e le procedure** di cui agli articoli 24 (Responsabilità del Titolare) e 25 (Protezione dei dati fin dalla progettazione e per impostazione predefinita) e le misure volte a garantire la sicurezza del trattamento di cui all'articolo 32;

la **notifica di una violazione** dei dati personali alle autorità di controllo e la comunicazione di tali violazioni dei dati personali all'interessato;

il **trasferimento di dati personali** verso paesi terzi o organizzazioni internazionali;

le **procedure stragiudiziali e di altro tipo per comporre le controversie** tra Titolari del trattamento e interessati in materia di trattamento, fatti salvi i diritti degli interessati ai sensi degli articoli 77 e 79.

Ai codici di condotta possono aderire anche i Titolari del trattamento o i Responsabili del trattamento che non sono soggetti al Regolamento quale garanzia adeguata nel quadro dei trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali e con impegno vincolante e azionabile, mediante strumenti contrattuali o di altro tipo giuridicamente vincolanti, di applicare le stesse adeguate garanzie anche per quanto riguarda i diritti degli interessati a norma dell'art. 46, par. 2, lett. e).

Il codice di condotta deve contenere dei **meccanismi che consentono all'organismo preposto al controllo di conformità del codice** ex art. 41, par. 1 e di cui al successivo paragrafo 16.1.2, **di effettuare il controllo obbligatorio** del rispetto delle norme del codice da parte dei Titolari del trattamento o dei Responsabili del trattamento che si impegnano ad applicarlo.

LA PROCEDURA DI APPROVAZIONE DEI CODICI DI CONDOTTA

Le associazioni e gli organismi rappresentanti le categorie di Titolari o Responsabili del trattamento che intendono elaborare, modificare o prorogare un codice di condotta devono **sottoporre il progetto di codice, la modifica o la proroga all'autorità di controllo competente ai sensi dell'art. 55, che esprime un parere sulla conformità dello stesso al Regolamento e approva tale progetto, modifica o proroga, se ritiene che il codice offra sufficienti ed adeguate garanzie.**

La procedura di approvazione del codice di condotta dipende dal luogo di svolgimento delle attività di trattamento.

Se il progetto di codice, la modifica o la proroga riguarda **attività di trattamento che si svolgono solo in uno Stato membro, l'autorità di controllo di tale Stato membro, dopo aver approvato il progetto, modifica o proroga del codice, provvede a registrarlo e pubblicarlo.**

Se invece il progetto di codice, la modifica o la proroga riguarda **attività di trattamento che si svolgono in vari Stati membri, l'autorità di controllo competente sottopone** il progetto di codice, la modifica o la proroga **al Comitato europeo per la protezione dei dati che formula un parere** sulla conformità al Regolamento o sulla previsione di adeguate garanzie nel caso di adesione al codice da parte di titolari o responsabili del trattamento che non sono soggetti al Regolamento.

In caso di parere positivo il Comitato trasmette il suo parere alla Commissione che, mediante atti di esecuzione adottati secondo la procedura d'esame, può decidere che il codice di condotta, della modifica o della proroga approvati hanno validità generale all'interno dell'Unione Europea.

La Commissione provvede a dare un'adeguata pubblicità dei codici approvati per i quali è stata decisa la validità generale all'interno dell'Unione Europea.

Tutti i codici di condotta, le modifiche e le proroghe approvati **sono raccolti in un registro** a cura **del Comitato** che provvede anche a **renderli pubblici** mediante mezzi appropriati.

IL MONITORAGGIO DEI CODICI DI CONDOTTA APPROVATI

Il **controllo della conformità con un codice di condotta approvato può essere effettuato da un organismo in possesso del livello adeguato di competenze** riguardo al contenuto del codice ed accreditato presso l'autorità di controllo competente.

Per poter essere accreditato dall'autorità di controllo competente, detto organismo deve soddisfare i seguenti requisiti:

aver **dimostrato** in modo convincente all'autorità di controllo competente **di essere indipendente e competente** riguardo al contenuto del codice di condotta;

aver **istituito delle procedure** che gli consentono di valutare l'ammissibilità dei Titolari e dei Responsabili del trattamento ad applicare il codice, di controllare che detti Titolari e Responsabili ne rispettino le disposizioni e di riesaminarne periodicamente il funzionamento;

aver istituito procedure e strutture atte a gestire i reclami relativi a violazioni del codice di condotta o il modo in cui il codice è stato o è attuato da un Titolare del trattamento o un Responsabile del trattamento ed a rendere dette procedure e strutture trasparenti per gli interessati e il pubblico;

aver dimostrato in modo convincente all'autorità di controllo competente **che i compiti e le funzioni** da esso svolti **non danno adito a conflitto di interessi**.

L'organismo **deve adottare opportune misure in caso di violazione del codice di condotta** da parte di un Titolare o Responsabile del trattamento, tra cui la sospensione o l'esclusione dal codice del Titolare del trattamento o del Responsabile del trattamento, **informando l'autorità di controllo** competente di tali misure e dei motivi della loro adozione.

L'**accreditamento dell'organismo può essere revocato dall'autorità di controllo** competente se le condizioni per l'accreditamento non sono, o non sono più, rispettate o se le misure adottate dall'organismo violano il Regolamento.

Il monitoraggio dei codici di condotta non si applica al trattamento effettuato da autorità pubbliche e da organismi pubblici.

I MECCANISMI DI CERTIFICAZIONE

Il Regolamento prevede l'istituzione di meccanismi di certificazione della protezione dei dati, nonché di sigilli e marchi di protezione dei dati quale strumento:

per i Titolari ed i Responsabili del trattamento soggetti al Regolamento per dimostrare la conformità dei trattamenti effettuati;

per i Titolari del trattamento o i Responsabili del trattamento che non sono soggetti al Regolamento per dimostrare la previsione di garanzie appropriate nel quadro dei trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali con impegno vincolante e azionabile, mediante strumenti contrattuali o di altro tipo giuridicamente vincolanti, di applicare le stesse adeguate garanzie anche per quanto riguarda i diritti degli interessati.

La certificazione, che è volontaria, non riduce comunque la responsabilità del Titolare o del Responsabile del trattamento riguardo alla conformità al Regolamento, restando impregiudicati i compiti e i poteri delle autorità di controllo competenti.

Ai sensi dell'art. 42, par. 5, la certificazione può essere **rilasciata dagli organismi di certificazione** disciplinati dall'art. 43 del Regolamento **o dall'autorità di controllo competente** in base a criteri approvati dalla stessa autorità di controllo o dal Comitato Europeo per la protezione dei dati e, in tale ultimo caso, ciò può risultare in una certificazione comune (il sigillo europeo per la protezione dei dati).

La certificazione è rilasciata al Titolare o al Responsabile del trattamento **per un periodo massimo di tre anni e può essere rinnovata** alle stesse condizioni purché continuino a essere soddisfatti i requisiti pertinenti.

La certificazione è revocata, se del caso, **dagli organismi di certificazione o dall'autorità di controllo competente**, a seconda dei casi, qualora non siano o non siano più soddisfatti i requisiti per la certificazione.

Tutti i meccanismi di certificazione e i sigilli e i marchi di protezione dei dati sono **raccolti in un registro a cura del Comitato** che li rende pubblici con qualsiasi mezzo appropriato.

Ai sensi dell'art. 43, **gli organismi di certificazione devono essere accreditati da uno o entrambi i seguenti organismi:**

dall'autorità di controllo competente ai sensi degli artt. 55 o 56;

dall'organismo nazionale di accreditamento designato in virtù del regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio[30] conformemente alla norma EN-ISO/IEC 17065/2012 e ai requisiti aggiuntivi stabiliti dall'autorità di controllo competente ai sensi degli articoli 55 o 56.

Ai fini del predetto accreditamento, gli organismi di certificazione devono:

aver dimostrato in modo convincente all'autorità di controllo competente di essere indipendenti e competenti riguardo al contenuto della certificazione;

essersi impegnati a rispettare i criteri di cui all'art. 42, par. 5, approvati dall'autorità di controllo competente ai sensi degli artt. 55 o 56 o dal Comitato, ai sensi dell'art. 63, che integrano quelli previsti dal regolamento (CE) n. 765/2008 e le norme tecniche che definiscono i metodi e le procedure degli organismi di certificazione;

aver istituito procedure per il rilascio, il riesame periodico e il ritiro delle certificazioni, dei sigilli e dei marchi di protezione dei dati;

30. NB Regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio, del 9 luglio 2008, che pone norme in materia di accreditamento e vigilanza del mercato per quanto riguarda la commercializzazione dei prodotti e che abroga il regolamento (CEE) n. 339/93. L'ente italiano di Accreditamento quale unico organismo nazionale autorizzato dallo Stato a svolgere attività di accreditamento è ACCREDIA, designato dal Governo il 22 dicembre 2009.

aver istituito procedure e strutture atte a gestire i reclami relativi a violazioni della certificazione o il modo in cui la certificazione è stata o è attuata dal Titolare del trattamento o dal responsabile del trattamento e a rendere dette procedure e strutture trasparenti per gli interessati e il pubblico; e

aver dimostrato in modo convincente all'autorità di controllo competente che i compiti e le funzioni da loro svolti non danno adito a conflitto di interessi.

L'accreditamento è rilasciato all'organismo di certificazione per un periodo massimo di cinque anni e può essere rinnovato alle stesse condizioni purché l'organismo di certificazione soddisfi i requisiti.

L'**accreditamento** di un organismo di certificazione **può essere revocato** dall'autorità di controllo competente o dall'organismo nazionale di accreditamento se le condizioni per l'accreditamento non sono, o non sono più, rispettate o se le misure adottate da un organismo di certificazione violano il Regolamento.

Gli **organismi di certificazione sono responsabili della corretta valutazione** circa il rilascio o la revoca della certificazione, fatta salva la responsabilità del Titolare o del Responsabile del trattamento riguardo alla conformità al Regolamento, e **devono trasmettere all'autorità di controllo competente i motivi del rilascio o della revoca della certificazione** richiesta.

La Commissione europea ha il potere di adottare atti delegati per precisare i requisiti di cui tenere conto per i meccanismi di certificazione della protezione dei dati, **nonché adottare atti di esecuzione per stabilire norme tecniche riguardanti i meccanismi di certificazione e i sigilli e marchi di protezione dei dati e le modalità per promuovere e riconoscere tali meccanismi di certificazione, i sigilli e marchi di protezione dei dati.**

Per completezza, è opportuno ricordare come il Garante per la protezione dei dati persoanli ed ACCREDIA, abbiano pubblicato un comunicato stampa congiunto il 18 Luglio 2017.

Nello specifico: "In particolare ACCREDIA e il Garante per la protezione dei dati personali ritengono necessario sottolineare - al fine di indirizzare correttamente le attività svolte dai soggetti a vario titolo interessati in questo ambito - che al momento le certificazioni di persone, nonché quelle emesse in materia di privacy o data protection eventualmente rilasciate in Italia, sebbene possano costituire una garanzia e atto di diligenza verso le parti interessate dell'adozione volontaria di un sistema di analisi e controllo dei principi e delle norme di riferimento, a legislazione vigente non possono definirsi "conformi agli artt. 42 e 43 del regolamento 2016/679", poiché devono ancora essere determinati i "requisiti aggiuntivi" ai fini dell'accreditamento degli organismi di certificazione e i criteri specifici di certificazione".

Per completezza si rimanda al link: http://www.accredia.it/UploadDocs/7180_DC2017SSV207.pdf, evidenziando come la formazione in ambito ISO/IEC 17024 a cui parrebbe riferirsi il comunicato, non alcuna attinenza con gli artt.42/43 del GDPR, che riguardano i meccanismi di certificazione delle aziende.

Di contro Accredia sottolinea come "-omissis- Organismo di certificazione accreditato da ACCREDIA a fronte della 17065:2012 per lo schema - omissis- , ha sviluppato lo schema, l'ISDP 10003:2015, applicabile a qualsiasi Titolare del trattamento, qualunque sia il settore di appartenenza ed a prescindere dal tipo di trattamento realizzato e che risponde ai requisiti previsti dal regolamento stesso sia in ambito nazionale che europeo. -omissis- è quindi il proprietario dello schema ISDP 10003:2015. Questo schema è già stato valutato con esito positivo da ACCREDIA, e può essere oggetto di accreditamento (ambito volontario) a favore di altri Organismi di Certificazione per lo schema ISO/IEC 17065." , fugando, di fatto, qualsiasi dubbio sulla liceità dell'accreditamento dello schema stesso.

L'iniziativa è stata realizzata grazie al supporto incondizionato di