

Allegato A
al decreto direttore n. ...del 00/00/2019

Data Protection Policy
Agenzia regionale di sanità
Modello organizzativo

INTRODUZIONE

Con l'entrata in vigore dal 25 maggio 2018 del nuovo Regolamento europeo sulla privacy la protezione dei dati trova oggi un nuovo impulso, nell'ottica della definizione di regole sostanziali più che formali.

L'Agenzia Regionale di Sanità, che per finalità istitutive è preposta al trattamento di dati sensibili, in ossequio ai principi sanciti dalla Comunità Europea e dal legislatore statale, intende procedere alla definizione di un sistema di tutela della privacy, nella convinzione che attraverso il rispetto dei dati della persona si può ottenere un risultato importante: quello della tutela della dignità dei cittadini.

Nell'ottica predetta, s'impone pertanto un impegno organizzativo che passerà attraverso azioni successive a breve, medio termine sino a giungere, in armonia con le scadenze dettate dal nuovo regolamento, alla definizione di un sistema di regole certe.

Si delineano, di seguito, i passaggi fondamentali di detto impegno:

1. AZIONI A BREVE TERMINE

- Introduzione del principio di Accountability, ovvero principio con il quale è onere dell'azienda o dell'ente dimostrare un atteggiamento proattivo nella salvaguardia del dato personale dell'utente;
- Nomina di un Data Protection Officer – Responsabile della sicurezza della Protezione dei Dati (DPR – RPD), ovvero di una nuova figura aziendale assolutamente indipendente dalla governance e deputata a sorvegliare l'osservanza degli obblighi sulla protezione dei dati posti in capo al titolare o al responsabile del trattamento;
- Istituzione e tenuta dei registri delle attività di trattamento;

2. AZIONI A MEDIO TERMINE

- Sicurezza dei trattamenti dei dati personali;
- Valutazione d'impatto sulla protezione dei dati;
- Segnalazione di violazione dei dati personali (data breach), ovvero estensione a tutti i Titolari e Responsabili dell'obbligo di comunicazione al Garante dell'avvenuta violazione dei dati personali;

L'intento è anche quello di permettere a tutti gli addetti di operare nel quadro d'indicazioni certe, che non devono essere intese come ulteriore appesantimento burocratico, ma come miglioramento della qualità del servizio offerto ai cittadini.

Il presente documento, che contiene le indicazioni del Titolare da impartire ai delegati del trattamento, si colloca nell'ambito delle azioni a breve termine sopra enunciate, ed ha lo scopo di avviare il processo di regolazione della materia. Le stesse sono impartite secondo la disciplina recata dal regolamento EU n. 2016/679.

In ultimo, al fine di agevolare gli operatori nell'attuazione della disciplina vigente nella materia trattata, la cui interpretazione risulta complessa in conseguenza dei molteplici dati di riferimento all'attività dell'Agenzia, contenuti nel testo delle disposizioni, insieme alle presenti indicazioni è sintetizzata un'analisi del **Regolamento Generale sulla Protezione dei Dati** - Regolamento Europeo UE 2016/679 corredata da alcune tavole che riassumono rispettivamente: gli obblighi derivanti all'ARS in ordine alla sua collocazione giuridica e gli obblighi derivanti ai singoli soggetti, nonché una modulistica semplificata riguardante:

- informativa

- fac simile atto di nomina del responsabile
- fac simile atto di nomina del sub responsabile
- fac simile atto di nomina autorizzati
- fac simile accordo tra titolari autonomi
- fac simile accordo fra contitolari
- fac simile accordo fra titolare e responsabile

IL DIRETTORE
Dott. Mario Braga

INDICE

1. *ARS: natura giuridica e organizzazione*
 - 1.1. *L'Agenzia: personale e risorse finanziarie*
 - 1.2. *Funzioni*

2. **IL NUOVO REGOLAMENTO EUROPEO**
 - 2.1. *Entrata in vigore*
 - 2.2. *Principi generali*
 - 2.3. *Il titolare. La responsabilizzazione del titolare*
 - 2.4. *I Soggetti delegati attuatori*
 - 2.5. *Specifiche attribuzioni al direttore*
 - 2.6. *I responsabili del trattamento*
 - 2.7. *Gli autorizzati*

3. **RESPONSABILE DELLA PROTEZIONE DEI DATI**
 - 3.1. *Soggetti obbligati*
 - 3.2. *Caratteristiche soggettive*
 - 3.3. *Compiti e responsabilità*
 - 3.4. *Ufficio del DPO*
 - 3.5. *Pareri del DPO*
 - 3.6. *Accesso civico generalizzato e ruolo DPO*

4. **ADEMPIMENTI VERSO GLI INTERESSATI**
 - 4.1. *L'informativa*
 - 4.2. *La raccolta del consenso*
 - 4.3. *Il riscontro nell'esercizio dei diritti*

5. **ADEMPIMENTI INTERNI**
 - 5.1 *Il trattamento dei dati*
 - 5.2 *Presupposti giuridici per ARS per trattamento dati*
 - 5.3 *Fattispecie tipiche.*
 - 5.3.1 *Fattispecie n. 1*
 - 5.3.2 *Fattispecie n. 2*
 - 5.3.3 *Fattispecie n. 3*
 - 5.4 *I registri delle attività di trattamento*
 - 5.5 *La valutazione di impatto privacy*
 - 5.6 *Il registro delle violazioni di dati personali (processo di Data Breach)*

6. **ALTRI ADEMPIMENTI**
 - 6.1. *IL trasferimento di dati all'estero*
 - 6.2. *Clausole contrattuali del titolare*

7. **SANZIONI**
 - 7.1 *GDPR: le sanzioni amministrative pecuniarie e/o penali*

8. **PROTEZIONE DEI DATI E RICERCA IN AMBITO SANITARIO**

9. **DIPOSIZIONI FINALI**

ALLEGATI:

- ALLEGATO 1 modello nomina responsabile
- ALLEGATO 2 modello nomina sub responsabile
- ALLEGATO 3 modello nomina autorizzati
- ALLEGATO 4 organigramma con nomine
- ALLEGATO 5 informativa_lavoro
- ALLEGATO 6 informativa_avviso
- ALLEGATO 7 informativa_bandi_concorsi
- ALLEGATO 8 informativa_dipendenti
- ALLEGATO 9 informativa_formazione
- ALLEGATO 10 informativa_generica_interessati
- ALLEGATO 11 informativa_iniziative_promozionali_forum_convegni
- ALLEGATO 12 informativa_Newsletteres
- ALLEGATO 13 informativa_portinerie
- ALLEGATO 14 informativa_Videsorveglianza
- ALLEGATO 15 DPA Titolare Responsabile-(sub responsabile)
- ALLEGATO 16 DPA Fra titolari autonomi,
- ALLEGATO 17 DPA di Contitolarità

Appendice normativa

Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali

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) (Testo rilevante ai fini del SEE)

WP 243 – Linee guida sui responsabili della protezione dei dati (DPO/RPD)

Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, wp248rev.01

1 ARS: NATURA GIURIDICA E ORGANIZZAZIONE

L'Agenzia Regionale di Sanità (ARS) è un ente di consulenza della Regione Toscana, dotato di autonomia amministrativa, organizzativa e contabile, che svolge prevalentemente attività di supporto scientifico in ambito socio-sanitario sia per la Giunta regionale che per il Consiglio regionale.

In particolare ARS svolge attività di studio e ricerca in materia di epidemiologia attraverso analisi, proposte e valutazioni che hanno come oggetto lo stato e i bisogni di salute dei cittadini toscani. Si occupa inoltre di verificare la qualità dei servizi socio-sanitari regionali e l'equità di accesso ai servizi stessi da parte della popolazione toscana, con l'obiettivo di promuoverne il miglioramento.

Con la propria attività di ricerca fornisce informazioni e strumenti a supporto della programmazione regionale e dei processi decisionali e di rinnovamento organizzativo, sia di livello regionale che locale. Secondo il combinato disposto degli articoli 82, 82-bis, 82-ter e 82-novies decies della suddetta l.r. 40/2005, l'Agenzia è autorizzata ad accedere a tutti i flussi di dati a carattere regionale attinenti alla salute e al benessere sociale, ovunque collocati, per scopi di ricerca scientifica, specificando i tipi di dati che possono essere trattati, le operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite.

E' stata istituita nel 1998 con la legge regionale n. 71 ed è stata poi riordinata con la l.r. n. 40 (Disciplina del servizio sanitario regionale) del 24 febbraio 2005 e successive modifiche, che ne ha fissato in via definitiva i compiti, le funzioni e la struttura organizzativa.

1.1 L'AGENZIA: PERSONALE E RISORSE FINANZIARIE

L'attuale assetto organizzativo dell'ARS prevede tre strutture operative: l'Osservatorio di Epidemiologia, l'Osservatorio per la Qualità e l'Equità e la Direzione.

L'ARS svolge le proprie funzioni attraverso strutture operative, cui è preposto un responsabile. La struttura operativa per l'esercizio delle funzioni tecnico-amministrative e scientifiche a carattere generale è denominata Direzione. Le strutture operative per l'esercizio delle funzioni scientifico-disciplinari, sono l'Osservatorio di epidemiologia e l'Osservatorio per la qualità e l'equità.

La Direzione accoglie tutte le attività trasversali di supporto agli organi nonché alle strutture operative dell'Agenzia per lo svolgimento delle sue funzioni istituzionali e scientifiche.

L'Osservatorio di epidemiologia raccoglie, elabora e sistematizza i dati utili a descrivere lo stato di salute della popolazione toscana, le dinamiche demografiche, la diffusione delle malattie, le azioni di prevenzione ed i bisogni di cura da esse derivanti per individuare fattori di rischio individuali, sociali e ambientali e per indirizzare e monitorare la programmazione sanitaria a livello aziendale e regionale. La mission è quella di fornire ai decisori le migliori conoscenze scientifiche disponibili per poter pianificare interventi tesi alla riduzione degli effetti sulla salute dei determinanti socio-economici di salute e delle esposizioni ambientali e per migliorare la qualità e l'efficacia dell'assistenza sanitaria.

L'Osservatorio per la qualità e l'equità contribuisce con le proprie attività al miglioramento della qualità dell'assistenza socio-sanitaria offerta in Toscana; la mission è quella di sviluppare, sia in modo sistematico che esplorativo, misure e indicatori relativi al funzionamento delle componenti

del Sistema Sanitario Regionale, al loro grado di risposta ai bisogni dei cittadini e agli esiti delle cure offerte, nella convinzione che solo informazioni accurate e tempestive possano supportare processi virtuosi di miglioramento consistenti.

Il personale in servizio al 31/12/2018 risulta essere di n. 56 dipendenti (compreso il personale a tempo determinato). La tabella seguente mette a confronto le differenze tra il personale in servizio in ARS, distinto tra le tre diverse strutture operative, con l'analogo quadro conoscitivo riferito al precedente biennio.

DISTRIBUZIONE PERSONALE ENTE									
Strutture	Al 31/12/2016			Al 31/12/2017			Al 31/12/2018		
	Comparto	Dirigenza	Totale	Comparto	Dirigenza	Totale	Comparto	Dirigenza	Totale
<i>Direzione</i>	28	1	29	28	1	29	29	1	30
<i>Osservatorio di Epidemiologia</i>	14	2	16	15	2	17	15	2	17
<i>Osservatorio Qualità e Equità</i>	7	0	8	7	1	8	8	1	9
TOTALE	49	3	52	50	4	54	52	4	56

1.2 Funzioni

L'ARS svolge le proprie funzioni attraverso distinte strutture operative, cui è preposto un responsabile. Le strutture operative possono essere articolate in settori, la cui responsabilità è attribuita a dirigenti.

La struttura operativa per l'esercizio delle funzioni tecnico-amministrative e scientifiche a carattere generale è denominata direzione. Le strutture operative per l'esercizio delle funzioni scientifico-disciplinari, sono, come detto in precedenza, l'osservatorio di epidemiologia e l'osservatorio per la qualità e l'equità. La responsabilità di tali strutture è affidata ad un coordinatore.

2. IL NUOVO REGOLAMENTO EUROPEO

2.1 Entrata in vigore

Il Regolamento (UE) 2016/679 del Parlamento europeo e del consiglio europeo 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 94/46/CE (regolamento generale sulla protezione dei dati) è stato pubblicato il 4 maggio 2016 nella Gazzetta Ufficiale dell'Unione Europea (GUUE) unitamente alla direttiva che regola i trattamenti dei dati personali nei settori della prevenzione, contrasto e repressione dei crimini. Il 5 maggio è entrata ufficialmente in vigore la direttiva, che dovrà essere recepita dagli Stati membri entro due anni. Il 24 maggio è entrato ufficialmente in vigore il Regolamento ed il testo è diventato definitivamente applicabile in via diretta in tutti i paesi UE a partire dal 25 maggio 2018.

2.2 Principi generali

Il trattamento dei dati personali deve essere attuato nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

Il trattamento dei dati personali è attuato assicurando un elevato livello di tutela dei diritti e delle libertà, nel rispetto dei principi di semplificazione, armonizzazione ed efficacia delle modalità previste per il loro esercizio.

I sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

Le modalità del trattamento devono essere attuate avendo riguardo a trattare i dati personali in modo lecito e secondo correttezza ed in via generale secondo il principio di pertinenza e non di eccedenza; gli stessi devono essere raccolti e registrati ed aggiornati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi; devono essere pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati; infine gli stessi devono essere conservati in una forma che consenta l'identificazione dell'interessato per un periodo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

I dati personali trattati in violazione della disciplina rilevante in materia, non possono essere utilizzati.

Il Regolamento si applica integralmente alle imprese situate fuori dell'Unione europea che offrono servizi o prodotti a persone che si trovano nel territorio dell'Unione europea. Tutte le aziende, ovunque stabilite, dovranno quindi rispettare le regole fissate dall'UE (Google, Facebook, Microsoft, Apple, ecc....).

Il Regolamento introduce regole più chiare in materia di informativa e di consenso, definisce i limiti al trattamento automatizzato dei dati personali, pone le basi per l'esercizio dei nuovi diritti, stabilisce criteri più rigorosi per il trasferimento dei dati al di fuori dell'UE e per i casi di violazione dei dati personali (*data breach*).

L'**informativa** diventa sempre di più uno strumento di trasparenza riguardo al trattamento dei dati personali e dell'esercizio dei diritti. Gli interessati dovranno sapere se i loro dati saranno trasmessi al di fuori dell'UE e con quali garanzie; così come dovranno sapere che hanno il diritto di revocare il consenso a determinati trattamenti, come quelli di marketing diretto.

Il **consenso** dell'interessato al trattamento dei dati personali dovrà essere, come oggi, preventivo ed inequivocabile, anche quando espresso tramite mezzi elettronici (ad esempio, selezionando un'apposita casella in un sito web).

Per trattare i dati sensibili, il Regolamento prevede che il consenso debba essere anche esplicito.

Viene esclusa ogni forma di consenso tacito (il silenzio, cioè, non equivale al consenso) oppure ottenuto proponendo ad un interessato una serie di opzioni già selezionate.

Il consenso potrà essere revocato in ogni momento. I trattamenti effettuati fino a quel momento dal titolare sulla base del consenso rimarranno comunque legittimi. I fornitori di servizi internet e i social media dovranno richiedere il consenso ai genitori o a chi esercita la potestà genitoriale per trattare i dati personali dei minori dei 16 anni.

Le decisioni che producono effetti giuridici (come la concessione di un prestito) non potranno essere basate esclusivamente sul trattamento automatizzato dei dati (ad esempio la profilazione).

Faranno eccezione i casi in cui l'interessato abbia rilasciato un consenso esplicito al trattamento automatizzato dei suoi dati, oppure questo tipo di trattamento risulti strettamente necessario per la definizione di un contratto o avvenga sulla base dei specifici obblighi di legge.

In ogni caso, sono previste garanzie per gli interessati, come il diritto di opporsi alla decisione adottata sulla base di un trattamento automatizzato o il diritto di ottenere anche l'intervento umano rispetto alla decisione stessa. Se il trattamento è finalizzato all'attività di marketing diretto, l'interessato ha sempre il diritto di opporsi alla profilazione.

Fra le principali novità del Regolamento c'è il cosiddetto sportello unico (**one stop shop**), che semplificherà la gestione dei trattamenti e garantirà un approccio uniforme.

Salvo casi specifici, le imprese stabilite in più Stati membri o che offrono prodotti e servizi in vari Paesi dell'UE, per risolvere possibili problematiche sull'applicazione e il rispetto del Regolamento potranno rivolgersi ad un solo interlocutore: cioè all'autorità di protezione dei dati del Paese dove si trova il loro stabilimento principale.

Le definizioni che conosciamo si aggiornano e se ne aggiungono di nuove:

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

2) «**trattamento**»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

7) «**titolare del trattamento**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

8) «**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;

Il Regolamento definisce caratteristiche soggettive e responsabilità del titolare e del responsabile del trattamento negli stessi termini di cui alla direttiva 95/46/CE (e quindi al Codice privacy italiano). Pur non prevedendo espressamente la figura dell'incaricato del trattamento (ex art. 30 Codice), il Regolamento non ne esclude la presenza in quanto fa riferimento a “persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile(si veda in particolare, art. 4, n. 10 del Reg.UE 2016/679).

9) «**security IT manager**»: figura implicitamente prevista dal GDPR, per garantire quanto previsto alla sezione dedicata alla “sicurezza dei dati personali” , per supportare il Titolare nei suoi compiti di supervisione e controllo delle misure di sicurezza adottate, per determinarne la loro adeguatezza nel tempo e per garantire il rispetto del principio di separazione delle responsabilità fra chi le misure le deve attuare, il Responsabile/i della sicurezza IT dell'organizzazione o il Responsabile del trattamento, e chi invece deve controllarle;

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

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

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

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

I nuovi principi applicabili al trattamento non si distaccano da quelli già introdotti dal Codice privacy. In particolare l'art. 5 del regolamento prevede che i dati personali debbano essere:

- 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»).

Inoltre il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di provarlo («**responsabilizzazione**»).

Il Regolamento infatti introduce un fondamentale nuovo concetto che è quello della responsabilizzazione (**accountability**) dei titolari del trattamento e promuove l'adozione di approcci che tengano conto costantemente del rischio che un determinato trattamento di dati personali possa comportare per i diritti e le libertà degli interessati.

Il titolare del trattamento dovrà sempre essere in grado di dimostrare di aver adottato un complessivo processo di misure giuridiche, organizzative, tecniche per la protezione dei dati personali, anche attraverso l'elaborazione di specifici modelli organizzativi, analoghi in certi modi a quelli utilizzati dal d.lgs n. 231/2001 (Con il d.lgs. 231 del 2001 è stato introdotto, per la prima volta nel nostro ordinamento, il principio della 'responsabilità amministrativa delle persone giuridiche' per i reati commessi dalle figure apicali, di vertice, e dalle persone sottoposte alla loro vigilanza (dipendenti, fornitori ecc.), nell'interesse o a vantaggio dell'ente stesso. Il decreto prevede, quale 'esimente', la possibilità di dotarsi di un Modello di Organizzazione, Gestione e Controllo e di un Organismo di Vigilanza. Il modello deve essere efficace e costantemente verificato ed aggiornato.

Il monitoraggio tecnologico è in carico al Security Manager che provvede:

- a) alla redazione e attuazione di un piano per le verifiche sulle misure di sicurezza messe in atto dai dirigenti responsabili dei sistemi e delle applicazioni IT o di fornitori esterni,

- b) alla verifica della rispondenza delle misure di sicurezza in essere alle linee guida emesse dal DPO
- c) alla relazione periodica sulle misure di sicurezza adottate evidenziando punti di criticità e proponendo remediation plan,

Il principio chiave della nuova protezione dei dati è il **by design**, ossia il garantire la protezione dei dati fin dalla fase di ideazione e progettazione di un trattamento o di un sistema e adottare comportamenti che consentano di prevenire possibili problematiche. A questo si aggiunge il principio del **by default** ovvero, per impostazione predefinita tutte le imprese dovrebbero trattare i dati personali nella misura necessaria per le finalità previste e per il periodo strettamente necessario a tali fini.

Quest'ultimo principio è già noto all'ordinamento italiano, basti pensare all'art. 3 del vecchio Codice secondo il quale *“I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.”*

2.3 Il titolare. La responsabilizzazione del titolare

Titolare dei trattamenti di dati personali, ai sensi dell'art. 4 n. 7 e art. 24 del Regolamento, è ARS, in nome del legale rappresentante pro tempore, il direttore, cui spetta l'adozione di misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al Regolamento. Spetta pertanto in particolare a ARS:

- adottare, nelle forme previste dal proprio ordinamento, gli atti necessari, anche con riferimento alle disposizioni del Codice per la protezione dei dati personali oggetto di prossimo adeguamento al Regolamento;
- designare il Responsabile della protezione dei dati;
- designare i soggetti delegati all'attuazione degli adempimenti previsti dalla normativa in materia di trattamento di dati personali;
- effettuare, a mezzo della struttura competente, apposite verifiche sulla osservanza delle vigenti disposizioni in materia di trattamento, ivi compreso i profili relativi alla sicurezza informatica, in collaborazione con il DPO designato;
- istruire i soggetti autorizzati al trattamento dei dati personali.

Strettamente legato ai nuovi principi introdotti dal Regolamento è il nuovo assetto della responsabilità del titolare del trattamento.

Si ricordano:

- l'art. 15 del Codice privacy secondo cui “1. Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile.2. Il danno non patrimoniale è risarcibile anche in caso di violazione dell'articolo 11.” –
- l'art. 2050 del codice civile rubricato Responsabilità per l'esercizio di attività pericolose “Chiunque cagiona danno ad altri nello svolgimento di un'attività pericolosa, per sua natura o per la natura dei mezzi adoperati, è tenuto al risarcimento, se non prova di avere adottato tutte le misure idonee a evitare il danno ”.
- l'articolo 167 codice privacy Trattamento illecito di dati: “1. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, operando in violazione di quanto disposto dagli articoli 123, 126 e 130 o dal provvedimento di cui all'articolo 129 arreca nocumento all'interessato, è

punito con la reclusione da sei mesi a un anno e sei mesi. 2. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, procedendo al trattamento dei dati personali di cui agli articoli 9 e 10 del Regolamento in violazione delle disposizioni di cui agli articoli 2 sexies e 2 octies, o delle misure di garanzia di cui all'articolo 2 septies ovvero operando in violazione delle misure adottate ai sensi dell'articolo 2 quinquiesdecies arreca nocimento all'interessato, è punito con la reclusione da uno a tre anni.”*omissis*...

Il Regolamento europeo, infatti, sposta il fulcro della normativa in materia di protezione dei dati personali dalla tutela dell'interessato e dei suoi diritti alla responsabilizzazione del titolare del trattamento. Occorre menzionare che accountability in inglese vuol dire "dover rendere conto del proprio operato", per cui è qualcosa in più della semplice responsabilizzazione.

Il titolare del trattamento, quindi, tenuto conto della natura, del contesto e della finalità del trattamento, dovrà garantire, ed essere in grado di dimostrarlo (appunto, renderne conto) che il trattamento è effettuato non solo in maniera conforme alla normativa ma in maniera tale da non determinare rischi e quindi gravare sui diritti e le libertà degli interessati. In tal senso si supera la concezione formalistica del passato, quando bastava avere il consenso per sentirsi in regola, perché oggi l'essere conformi al regolamento non è più sufficiente, in quanto il titolare ha sempre la responsabilità di tutelare l'interessato e la collettività dai rischi impliciti del trattamento. Infine, non è sufficiente adottare misure di conformità alle norme, ma occorre anche documentarle (principio di trasparenza) e garantirne l'efficacia.

Il regolamento europeo propone un approccio basato sul rischio, inteso come misura delle conseguenze del trattamento sui diritti e le libertà dell'interessato. In tal senso il titolare dovrà innanzitutto progettare i trattamenti fin dall'inizio (privacy by design e by default) in modo da limitare il più possibile i rischi, eventualmente procedendo ad una valutazione di impatto preventiva, ed adottando le misure di sicurezza ritenute adeguate. Anche qui si nota la centralità del ruolo del titolare che opera da sé tutte queste valutazioni, salvo controlli ex post dell'autorità di controllo, e decide in autonomia le misure da adottare, e quindi le modalità e i limiti del trattamento, alla luce dei principi previsti dal regolamento.

In tale prospettiva l'adozione di codici di condotta o certificazioni può essere un mezzo per dimostrare la conformità.

Obblighi

Tra gli obblighi imposti al titolare dal principio di responsabilizzazione abbiamo:

- progettazione del trattamento limitando i rischi e con la privacy per impostazione predefinita;
- eventuale valutazione di impatto (DPIA) del trattamento;
- adozione delle misure di sicurezza adeguate in base al rischio;
- formazione del personale;
- designazione di responsabili che forniscano garanzie sufficienti;
- nomina del DPO;
- nomina del Security IT Manager;
- trasparenza e informazione agli interessati;
- notifica delle violazioni dei dati alle autorità di controllo;
- tutele per i trasferimenti dei dati all'estero;
- documentazione delle attività di trattamento.

Il regolamento europeo dedicato tre articoli all'argomento:

Articolo 25 Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, 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.

2. Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, 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 della persona fisica.

3. Un meccanismo di certificazione approvato ai sensi dell'articolo 42 può essere utilizzato come elemento per dimostrare la conformità ai requisiti di cui ai paragrafi 1 e 2 del presente articolo.

Articolo 82 Diritto al risarcimento e responsabilità

1. Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento.

2. Un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento. Un responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento.

3. Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, a norma del paragrafo 2 se dimostra che l'evento dannoso non gli è in alcun modo imputabile.

4. Qualora più titolari del trattamento o responsabili del trattamento oppure entrambi il titolare del trattamento e il responsabile del trattamento siano coinvolti nello stesso trattamento e siano, ai sensi dei paragrafi 2 e 3, responsabili dell'eventuale danno causato dal trattamento, ogni titolare del trattamento o responsabile del trattamento è responsabile in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato.

5. Qualora un titolare del trattamento o un responsabile del trattamento abbia pagato, conformemente al paragrafo 4, l'intero risarcimento del danno, tale titolare del trattamento o responsabile del trattamento ha il diritto di reclamare dagli altri titolari del trattamento o responsabili del trattamento coinvolti nello stesso trattamento la parte del risarcimento corrispondente alla loro parte di responsabilità per il danno conformemente alle condizioni di cui al paragrafo 2.

6. Le azioni legali per l'esercizio del diritto di ottenere il risarcimento del danno sono promosse dinanzi alle autorità giurisdizionali competenti a norma del diritto dello Stato membro di cui all'articolo 79, paragrafo 2.

Articolo 83 Condizioni generali per infliggere sanzioni amministrative pecuniarie

1. Ogni autorità di controllo provvede affinché le sanzioni amministrative pecuniarie inflitte ai sensi del presente articolo in relazione alle violazioni del presente regolamento di cui ai paragrafi 4, 5 e 6 siano in ogni singolo caso effettive, proporzionate e dissuasive.

2. Le sanzioni amministrative pecuniarie sono inflitte, in funzione delle circostanze di ogni singolo caso, in aggiunta alle misure di cui all'articolo 58, paragrafo 2, lettere da a) a h) e j), o in luogo di tali misure. Al momento di decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa in ogni singolo caso si tiene debito conto dei seguenti elementi:

a) 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;

d) il grado di responsabilità del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto ai sensi degli articoli 25 e 32;

e) eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento;

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

g) le categorie di dati personali interessate dalla violazione;

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;

i) qualora siano stati precedentemente disposti provvedimenti di cui all'articolo 58, paragrafo 2, nei confronti del titolare del trattamento o del responsabile del trattamento in questione relativamente allo stesso oggetto, il rispetto di tali provvedimenti;

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

k) eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione.

3. Se, in relazione allo stesso trattamento o a trattamenti collegati, un titolare del trattamento o un responsabile del trattamento viola, con dolo o colpa, varie disposizioni del presente regolamento, l'importo totale della sanzione amministrativa pecuniaria non supera l'importo specificato per la violazione più grave.

4. In conformità del paragrafo 2, la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie fino a 10 000 000 EUR, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore:

a) gli obblighi del titolare del trattamento e del responsabile del trattamento a norma degli articoli 8, 11, da 25 a 39, 42 e 43;

b) gli obblighi dell'organismo di certificazione a norma degli articoli 42 e 43;

c) gli obblighi dell'organismo di controllo a norma dell'articolo 41, paragrafo 4;

5. In conformità del paragrafo 2, la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie fino a 20 000 000 EUR, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore:

a) i principi di base del trattamento, comprese le condizioni relative al consenso, a norma degli articoli 5, 6, 7 e 9;

b) i diritti degli interessati a norma degli articoli da 12 a 22;

c) i trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale a norma degli articoli da 44 a 49;

d) qualsiasi obbligo ai sensi delle legislazioni degli Stati membri adottate a norma del capo IX;

e) l'inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'autorità di controllo ai sensi dell'articolo 58, paragrafo 2, o il negato accesso in violazione dell'articolo 58, paragrafo 1.

6. In conformità del paragrafo 2 del presente articolo, l'inosservanza di un ordine da parte dell'autorità di controllo di cui all'articolo 58, paragrafo 2, è soggetta a sanzioni amministrative pecuniarie fino a 20 000 000 EUR, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

7. Fatti salvi i poteri correttivi delle autorità di controllo a norma dell'articolo 58, paragrafo 2, ogni Stato membro può prevedere norme che dispongano se e in quale misura possono essere inflitte sanzioni amministrative pecuniarie ad autorità pubbliche e organismi pubblici istituiti in tale Stato membro.

8. L'esercizio da parte dell'autorità di controllo dei poteri attribuiti dal presente articolo è soggetto a garanzie procedurali adeguate in conformità del diritto dell'Unione e degli Stati membri, inclusi il ricorso giurisdizionale effettivo e il giusto processo.

9. Se l'ordinamento giuridico dello Stato membro non prevede sanzioni amministrative pecuniarie, il presente articolo può essere applicato in maniera tale che l'azione sanzionatoria sia avviata dall'autorità di controllo competente e la sanzione pecuniaria sia irrogata dalle competenti autorità giurisdizionali nazionali, garantendo nel contempo che i mezzi di ricorso siano effettivi e abbiano effetto equivalente alle sanzioni amministrative pecuniarie irrogate dalle autorità di controllo. In ogni caso, le sanzioni pecuniarie irrogate sono effettive, proporzionate e dissuasive. Tali Stati membri notificano alla Commissione le disposizioni di legge adottate a norma del presente paragrafo al più tardi entro 25 maggio 2018 e comunicano senza ritardo ogni successiva modifica.

2.4 I Soggetti delegati

Sono designati quali soggetti attuatori degli adempimenti necessari per la conformità dei trattamenti di dati personali effettuati da ARS in esecuzione del regolamento:

- il coordinatore dell'osservatorio di epidemiologia;
- il coordinatore dell'osservatorio per la qualità e l'equità;
- i dirigenti;
- le posizioni organizzative.

Relativamente ai trattamenti di dati personali trasversali a più strutture si applica il criterio della prevalenza,

Di seguito, sono indicati i compiti affidati ai soggetti delegati:

- a) verificare la legittimità dei trattamenti di dati personali effettuati dalla struttura di riferimento;
- b) disporre, in conseguenza alla verifica di cui alla lett. a) le modifiche necessarie al trattamento perché lo stesso sia conforme alla normativa vigente ovvero disporre la cessazione di qualsiasi trattamento effettuato in violazione alla stessa;
- c) adottare soluzioni di privacy by design e by default;
- d) tenere costantemente aggiornato il registro delle attività di trattamento per la struttura di competenza; predisporre le informative relative al trattamento dei dati personali nel rispetto dell'art. 13 del Regolamento;
- e) individuare i soggetti autorizzati a compiere operazioni di trattamento (di seguito anche "incaricati") fornendo agli stessi istruzioni per il corretto trattamento dei dati, sovrintendendo e vigilando sull'attuazione delle istruzioni impartite; tale individuazione deve essere effettuata in aderenza alle indicazioni contenute nel presente documento ed, in particolare, facendo espresso richiamo alle policy in materia di sicurezza informatica e protezione dei dati personali;
- f) predisporre ogni adempimento organizzativo necessario per garantire agli interessati l'esercizio dei diritti previsti dalla normativa;
- g) provvedere, anche tramite gli incaricati, a dare riscontro alle istanze degli interessati inerenti l'esercizio dei diritti previsti dalla normativa;
- h) disporre l'adozione dei provvedimenti imposti dal Garante;
- i) collaborare con l'ufficio del DPO al fine di consentire allo stesso l'esecuzione dei compiti e delle funzioni assegnate;
- j) adottare, se necessario, specifici disciplinari tecnici di settore, anche congiuntamente con altri soggetti delegati all'attuazione, per stabilire e dettagliare le modalità di effettuazione di particolari trattamenti di dati personali relativi alla propria area di competenza;

- k) individuare, negli atti di costituzione di gruppi di lavoro comportanti il trattamento di dati personali, i soggetti che effettuano tali trattamenti quali incaricati, specificando, nello stesso atto di costituzione, anche le relative istruzioni;
- l) garantire al DPO e all'ufficio del DPO i necessari permessi di accesso ai dati ed ai sistemi per l'effettuazione delle verifiche di sicurezza, anche a seguito di incidenti di sicurezza;
- m) designare gli amministratori di sistema in aderenza alle norme vigenti in materia;
- n) collaborare con l'ufficio del DPO alla preventiva valutazione d'impatto ai sensi dell'art. 35 del Regolamento, nei casi in cui un trattamento, allorché preveda in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

Nell'attuazione dei compiti sopra indicati i soggetti delegati possono acquisire il parere del DPO nei casi e con le modalità specificate nel seguito. Fermo restando che la responsabilità delle attività sopraindicate rimane in ogni caso in capo al soggetto delegato attuatore, in ragione del fatto che non sono ascrivibili a funzioni di direzione, coordinamento generale e controllo, in base ai principi generali relativi all'istituto della delega, sono eventualmente subdelegabili i compiti di cui alle lettere a), b), e), g), i). Tali compiti sono delegabili mediante formale provvedimento.

Secondo la disciplina recata dall'art. 82 *novies decies, comma 2* della l.r. n. 40/2005 e successive modificazioni, i coordinatori degli Osservatori sono i Responsabili del trattamento dei dati personali (comuni, sensibili e giudiziari) effettuati all'interno della rispettiva struttura e per l'ambito di competenza.

Tenuto conto dell'assetto dell'Agenzia, non è possibile individuare un soggetto delegato Di trattamenti afferenti alla Direzione.

Infatti, il dirigente del settore amministrazione è delegato per tutti i trattamenti relativi a contabilità, bilancio, acquisti di forniture e servizi.

Sarà direttamente il titolare avere la responsabilità dei trattamenti afferenti alle risorse umane, progetti e convenzioni, attività giudiziale e stragiudiziale ed a mettere in atto gli adempimenti necessari.

I delegati e i relativi ambiti di competenza sono specificatamente indicati nelle tabelle che seguono:

DELEGATI

STRUTTURE/UFFICI	DELEGATO	AMBITI DI COMPETENZA
<p style="text-align: center;">Direzione:</p> <ul style="list-style-type: none"> - P.O. Pianificazione, programmazione e controllo - Settore Amministrazione 	<p style="text-align: center;">Dirigente settore amministrazione (solo per lettere c), d), k))</p>	<ul style="list-style-type: none"> a) b) c) <i>Nell'ambito dei dati trattati all'interno della struttura di riferimento:</i> d) e) <i>dati comuni/ sensibili relativi ai componenti degli Organi e alla gestione del rapporto con gli stessi e l'Agenzia;</i> f) <i>dati comuni/ sensibili connessi ad assunzioni, alla stipula di contratti di diritto privato e alla gestione delle risorse umane (compenso, collocamento obbligatorio, assicurazioni integrative, concessione di 1/5 dello stipendio, procedure di conciliazione in materia di rapporto di lavoro, gestione cause di lavoro)</i> g) <i>dati relativi all'instaurazione e gestione dei rapporti contrattuali con terzi (individuazione del contraente, visura camerale, sottoscrizione contratto ecc;)</i> h) <i>dati relativi alla gestione ai fini contabili di indennità e retribuzioni agli organi e al personale</i> i) <i>dati comuni/ sensibili/ giudiziari per la gestione delle cause stragiudiziali</i> j) <i>dati comuni/ sensibili/ giudiziari relativi a istruttoria contenzioso giudiziale (affidamento difesa ARS a soggetti esterni, affidamento difesa ARS all'Avvocatura regionale)</i> k) <i>protocollo</i>

STRUTTURE/UFFICI	DELEGATO	AMBITI DI COMPETENZA
<p style="text-align: center;">Direzione:</p> <ul style="list-style-type: none"> - P.O. Information and Communications Technology - P.O. Soluzioni web, data visualization e documentazione scientifica 	-	<ul style="list-style-type: none"> a) flussi informativi analitici concernenti i ricoveri ospedalieri, l'erogazione delle prestazioni specialistiche ambulatoriali, di riabilitazione, di assistenza medica convenzionata, di assistenza farmaceutica territoriale e in regime ospedaliero, di trasporto sanitario, le anagrafi egli assistiti, le esenzioni per patologia ed invalidità, i certificati di assistenza al parto, le dimissioni per aborto spontaneo e le interruzioni volontarie di gravidanza; b) flussi informativi riguardanti le attività gestionali ed economiche del servizio sanitario e socio-sanitario regionale, nonché i dati di attività e di struttura sanitaria e socio-sanitaria pubblica e privata; c) flussi attinenti servizi di elaborazione dati e di verifica di qualità delle aziende sanitarie e delle istituzioni private; d) flussi informativi concernenti i dati sulla struttura della popolazione regionale, sull'anagrafe dei residenti, sugli stili di vita, sui fenomeni sociali, sui bisogni reali e sulle risorse; e) archivi delle malattie infettive, archivio regionale AIDS; f) registro regionale dei difetti congeniti, di mortalità, di dialisi, delle vaccinazioni, dei tumori; g) registro INAIL degli infortuni e delle malattie professionali; h) altri flussi informativi analitici che abbiano ad oggetto l'attività ospedaliera, le prestazioni sanitarie, socio-sanitarie e sociali erogate sul territorio, le prestazioni di riabilitazione, ulteriori archivi e registri di patologia.

STRUTTURE/UFFICI	DELEGATO	AMBITI DI COMPETENZA
<p align="center">OSSERVATORIO DI EPIDEMIOLOGIA</p> <ul style="list-style-type: none"> - P.O. Farmaco epidemiologia - P.O. Ambiente e Salute - P.O. Gestione dati sanitari <p>SETTORE SOCIALE:</p> <ul style="list-style-type: none"> - P.O. Malattie infettive e salute di genere - P.O. Diseguaglianze e stato di salute <p>SETTORE SANITARIO:</p> <ul style="list-style-type: none"> - P.O. Epidemiologia per la sanità pubblica e servizi socio-sanitari 	<p>Coordinatore</p>	<p>Nell'ambito dei dati trattati per progetti/programmi di pertinenza degli 'Osservatori, o per trattamenti effettuati da settori/uffici con funzioni trasversali:</p> <p><i>i) flussi informativi analitici concernenti i ricoveri ospedalieri, l'erogazione delle prestazioni specialistiche ambulatoriali, di riabilitazione, di assistenza medica convenzionata, di assistenza farmaceutica territoriale e in regime ospedaliero, di trasporto sanitario, le anagrafi egli assistiti, le esenzioni per patologia ed invalidità, i certificati di assistenza al parto, le dimissioni per aborto spontaneo e le interruzioni volontarie di gravidanza;</i></p> <p><i>j) flussi informativi riguardanti le attività gestionali ed economiche del servizio sanitario e socio-sanitario regionale, nonché i dati di attività e di struttura sanitaria e socio-sanitaria pubblica e privata;</i></p> <p><i>k) flussi attinenti servizi di elaborazione dati e di verifica di qualità delle aziende sanitarie e delle istituzioni private;</i></p> <p><i>l) flussi informativi concernenti i dati sulla struttura della popolazione regionale, sull'anagrafe dei residenti, sugli stili di vita, sui fenomeni sociali, sui bisogni reali e sulle risorse;</i></p> <p><i>m) archivi delle malattie infettive, archivio regionale AIDS;</i></p> <p><i>n) registro regionale dei difetti congeniti, di mortalità, di dialisi, delle vaccinazioni, dei tumori;</i></p> <p><i>o) registro INAIL degli infortuni e delle malattie professionali;</i></p> <p><i>p) altri flussi informativi analitici che abbiano ad oggetto l'attività ospedaliera, le prestazioni sanitarie, socio-sanitarie e sociali erogate sul territorio, le prestazioni di riabilitazione, ulteriori archivi e registri di patologia.</i></p>
<p align="center">OSSERVATORIO PER LA QUALITÀ E L'EQUITÀ</p> <ul style="list-style-type: none"> - P.O. Sistemi di valutazione della qualità - P.O. Reti cliniche e cure integrate 	<p>Coordinatore</p>	

2.5 Specifiche attribuzioni al direttore

Al direttore spetta, inoltre:

- l'adozione di policy in materia di privacy (<https://www.ars.toscana.it/privacy-policy.html>) e sicurezza informatica, con particolare riferimento all'utilizzo, alla sicurezza delle risorse informatiche e allo sviluppo delle applicazioni informatiche, da aggiornare periodicamente, ogni qualvolta l'evoluzione tecnica o normativa lo renda necessario;
- la sottoscrizione degli atti di notifica e di consultazione preventiva al Garante;
- la notifica e la comunicazione delle violazioni dei dati personali all'autorità di controllo ai sensi degli artt. 33 e 34 del Regolamento.

2.6 I responsabili del trattamento

Sono designati responsabili del trattamento di dati personali i soggetti esterni ad ARS che siano tenuti, a seguito di convenzione, contratto, verbale di aggiudicazione o provvedimento di nomina, ad effettuare trattamenti di dati personali per conto del titolare. Pertanto, qualora occorra affidare un incarico comportante anche trattamenti di dati personali, la scelta del soggetto deve essere effettuata valutando anche l'esperienza, la capacità e l'affidabilità in materia di protezione dei dati personali del soggetto cui affidare l'incarico, affinché lo stesso soggetto sia in grado di fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo della sicurezza. Attesa la natura negoziale delle designazioni dei responsabili del trattamento, questa deve essere effettuata con atto giuridico ai sensi dell'art. 37 del GDPR, all'interno di contratti o convenzioni e, in ogni caso, in costanza di formazione del rapporto contrattuale, in aderenza ai fac-simili messi a disposizione dalla struttura competente in materia di protezione dei dati. **(ALLEGATO 1 modello nomina responsabile).**

Il GDPR ha introdotto una figura non presente nella precedente disciplina, in quanto consente la nomina di sub responsabili del trattamento da parte di un responsabile (si veda l'articolo 28, paragrafo 4)), per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano titolare e responsabile primario; quest'ultimo risponde dinanzi al titolare dell'inadempimento dell'eventuale sub responsabile, anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso "non gli è in alcun modo imputabile" (si veda art. 82, paragrafo 1 e paragrafo 3).

ALLEGATO 2 modello nomina sub responsabile).

2.7 Gli autorizzati.

Il GDPR pur non prevedendo espressamente la figura dell'incaricato

Sono autorizzati al compimento alle operazioni di trattamento dei dati i soggetti delegati di cui al precedente paragrafo, i Responsabili di posizione organizzativa da loro delegati ai sensi della presente disciplina, che conformano i loro trattamenti alle policy aziendali in materia di protezione dei dati personali e alle istruzioni di seguito riportate:

- sono trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento;
- sono verificati legittimità e correttezza dei trattamenti, verificando, in particolare, i rischi che gli stessi presentano e la natura dei dati personali da proteggere.

Sono, altresì, autorizzati tutti i soggetti che effettuino operazioni di trattamento, dipendenti e collaboratori a qualsiasi titolo e che operano sotto la diretta autorità del Titolare o dei soggetti delegati. Tali soggetti devono essere da questi formalmente autorizzati. Gli autorizzati (ex incaricati) sono quindi designati:

- tramite individuazione nominativa (nome e cognome) delle persone fisiche. In questo caso occorre specificare, per ciascun nominativo, i trattamenti che lo stesso è autorizzato ad effettuare; (**ALLEGATO 3 modello nomina autorizzati**)

- tramite assegnazione funzionale della persona fisica all'unità organizzativa di minori dimensioni, qualora la persona fisica effettui tutti i trattamenti individuati puntualmente per tale unità.

Per quanto riguarda la nomina degli autorizzati si veda l'organigramma ARS allegato. (**ALLEGATO 4 organigramma con nomine**)

La designazione scritta deve inoltre contenere le istruzioni impartite agli incaricati del trattamento. Tali istruzioni, oltre a riguardare eventuali aspetti di dettaglio da diversificare in relazione alle specificità dei singoli trattamenti, devono quanto meno contenere un espresso richiamo alle policy di ARS in materia di sicurezza informatica e protezione dei dati personali.

I soggetti delegati sono tenuti a nominare uno o più autorizzati secondo le procedure descritte nel presente paragrafo e con l'atto di nomina vengono loro attribuiti i profili di autorizzazione indicati nelle tabelle che seguono.

Gli autorizzati sono suddivisi a seconda dell'unità operativa di riferimento fra amministratori ed utenti afferenti alle strutture scientifiche (osservatori) e amministratori ed utenti che afferiscono alle strutture amministrative (direzione e settore amministrazione).

Gli amministratori di sistema sono stati specificatamente nominati ed individuati nelle tre unità di personale della PO Information and Communications Technology (ITC) e nei soggetti che pur non essendo informatici e non svolgendo trattamenti inerenti la funzione istituzionale dell'Agenzia, svolgono attività per le quali necessitano di un raggio di azione ampio, inserendosi nella

PROFILI PER AUTORIZZATI

Amministratore di Sistema (AM): Gestisce il sistema operativo dell'elaboratore (Server o PC) che ospita il Database, eseguendo una serie di operazioni tecniche: dalla configurazione generale al controllo dei diversi momenti di attività (atto di nomina: nota del Presidente ARS del 6 febbraio 2009, prot. n. 267).

Amministratore di banca dati (database) (ABDC e AMBDS): Responsabile della progettazione, del controllo e della gestione del database e delle sue prestazioni, dell'affidabilità e delle autorizzazioni all'accesso.

Utente di Database (UB): Per mezzo di un linguaggio interattivo o tramite interfacce opportune, esegue applicazioni predefinite e interrogazioni sul database che non ne comportano la modifica, sia in termini di struttura che di contenuti.

Operatore inserimento dati (OID): Attraverso opportune interfacce, messe a disposizione dall'Amministratore di banca dati, inserisce i dati nel Database.

Utente di controllo (UC): nell'esercizio delle funzioni di indirizzo e controllo e verifica attribuito dalla legge agli organi dell'agenzia, svolge consultazione dati pseudoanonimizzati

AMMINISTRATORI

PROFILO	STRUTTURA / SETTORE	TIPOLOGIA DATI TRATTATI	OPERAZIONI
<p>A) AMMINISTRATORE BANCA DATI CENTRALE</p> <p>Detto profilo è attribuito per amministrare la banca dati centrale</p>	<p>P.O. Information and Communicati ons Technology</p> <p>P.O. Soluzioni web, data visualization e documentazio ne scientifica</p> <p>P.O. Farmaco epidemiologia</p> <p>P.O. Ambiente e Salute</p> <p>P.O. Gestione dati sanitari</p> <p>DIRIGENTE SETTORE SOCIALE</p> <p>P.O. Malattie infettive e salute di genere</p> <p>P.O. Diseguaglianz e e stato di salute</p> <p>DIRIGENTE SETTORE SANITARIO:</p> <p>P.O. Epidemiologi a per la sanità pubblica e servizi socio- sanitari</p> <p>P.O. Sistemi di valutazione della qualità</p> <p>P.O. Reti cliniche e cure integrate</p>	<p>DATI COMUNI DATI SENSIBILI</p>	<p>1) Raccolta:</p> <p>a) diretta presso l'interessato;</p> <p>b) utilizzo di archivi regionali;</p> <p>c) acquisizione archivi da soggetti terzi (pubblici o privati).</p> <p>2) Registrazione</p> <p>3) Organizzazione</p> <p>4) Conservazione</p> <p>5) Consultazione</p> <p>6) Elaborazione</p> <p>7) Modificazione</p> <p>8) Selezione</p> <p>9) Estrazione</p> <p>10) Raffronto</p> <p>11) Utilizzo</p> <p>12) Interconnessione</p> <p>13) Blocco</p> <p>14) Comunicazione (autoriz- zazione delegato</p> <p>15) Diffusione (autorizzazione Responsabile)</p> <p>16) Gestione della modalità di accesso</p> <p>17) Cancellazione</p> <p>18) Distruzione</p>

PROFILO	STRUTTURA / SETTORE	TIPOLOGIA DATI TRATTATI	OPERAZIONI
<p>B) AMMINISTRATORE DI SISTEMA</p> <p><i>Detto profilo è attribuito per amministrare tutte le banche dati presenti sugli elaboratori elettronici dell'ARS</i></p>	<p>P.O. Information and Communications Technology</p>	<p>DATI COMUNI DATI SENSIBILI</p>	<ol style="list-style-type: none"> 1) Raccolta <ol style="list-style-type: none"> a) diretta presso l'interessato; b) utilizzo di archivi regionali; c) acquisizione archivi da soggetti terzi (pubblici o privati). 2) Registrazione 3) Organizzazione 4) Conservazione 5) Consultazione 6) Elaborazione 7) Modificazione 8) Selezione 9) Estrazione 10) Raffronto 11) Utilizzo 12) Interconnessione 13) Blocco 14) Comunicazione (autorizzazione Responsabile) 15) Diffusione (autorizzazione delegato) 16) Gestione della modalità di accesso 17) Cancellazione 18) Distruzione

PROFILO	STRUTTURA / SETTORE	TIPOLOGIA DATI TRATTATI	OPERAZIONI
<p>C) AMMINISTRATO RE BANCA DATI SPECIFICA OSS</p> <p><i>Detto profilo è attribuito per amministrare una banca dati specifica diversa da quella centrale</i></p>	<p>P.O. Gestione dati sanitari o P.O. Soluzioni web, data visualization e documentazio ne scientifica</p> <p>PO degli osservatori responsabile scientifico del trattamento</p>	<p>DATI COMUNI DATI SENSIBILI</p>	<ol style="list-style-type: none"> 1) Raccolta <ol style="list-style-type: none"> a) diretta presso l'interessato; b) utilizzo di archivi regionali; c) acquisizione archivi da soggetti terzi (pubblici o privati). 2) Registrazione 3) Organizzazione 4) Conservazione 5) Consultazione 6) Elaborazione 7) Modificazione 8) Selezione 9) Estrazione 10) Raffronto 11) Utilizzo 12) Interconnessione con altri dati 13) Blocco 14) Comunicazione (autorizzazione Responsabile) 15) Diffusione (autorizzazione Responsabile) 16) Gestione delle modalità di accesso 17) Cancellazione 18) Distruzione

UTENTI OSSERVATORI/STRUTTURE TRASVERSALI

PROFILO	STRUTTURA / SETTORE	TIPOLOGIA DATI TRATTATI	OPERAZIONI
<p>D) UTENTE BANCA DATI CENTRALE</p> <p><i>Detto profilo è attribuito agli utenti della banca dati centrale</i></p>	<p>Tutti gli autorizzati degli OSSERVATORI I</p> <p>Tutti gli autorizzati della P.O. Gestione dati sanitari</p> <p>Tutti gli autorizzati della P.O. Gestione dati sanitari</p> <p>Tutti gli autorizzati della P.O. Soluzioni web, data visualization e documentazione scientifica</p>	<p>DATI COMUNI DATI SENSIBILI</p>	<ol style="list-style-type: none"> 1) Consultazione 2) Elaborazione 3) Selezione 4) Estrazione 5) Raffronto 6) Utilizzo 7) Interconnessione con altri archivi 8) Comunicazione (autorizzazione Responsabile) 9) Diffusione (autorizzazione Responsabile)
<p>E) UTENTE BANCA DATI SPECIFICA OSS</p> <p><i>Detto profilo è attribuito agli utenti di una banca dati specifica diversa da quella centrale</i></p>	<p>Tutti gli autorizzati degli OSSERVATORI I</p> <p>P.O. Gestione dati sanitari</p>	<p>DATI COMUNI DATI SENSIBILI</p>	<ol style="list-style-type: none"> 1) Consultazione 2) Elaborazione 3) Selezione 4) Estrazione 5) Raffronto 6) Utilizzo 7) Interconnessione con altri archivi 8) Comunicazione (autorizzazione delegato) 9) Diffusione (autorizzazione Responsabile)

UTENTI AMMINISTRATIVI

PROFILO	STRUTTURA/ SETTORE	TIPOLOGIA DATI	OPERAZIONI
F) AMMINISTRAT ORE BANCA DATI SPECIFICA amm	<p>DIRIGENTE SETTORE AMMINISTR AZIONE</p> <p>P.O. Pianificazione , programmazi one e controllo</p>	DATI SENSIBILI DATI GIUDIZIARI	<p>1. Raccolta: a) diretta presso l'interessato; b) acquisizione archivi da altri soggetti esterni (pubblici o privati)</p> <p>2. Registrazione 3. Organizzazione 4. Conservazione 5. consultazione 6. Elaborazione 7. Modificazione 8. Selezione 9. Estrazione 10. Raffronto 11. Utilizzo 12. Blocco 13. Comunicazione 14. Diffusione 15. Cancellazione 16. Distruzione</p>
G) UTENTE BANCA DATI SPECIFICA amm	<p>P.O. Pianificazione, programmazione e controllo</p> <p>Tutti gli autorizzati della DIREZIONE</p>		<p>1. Raccolta: a) diretta presso l'interessato; b) acquisizione archivi da altri soggetti esterni (pubblici o privati)</p> <p>2. Registrazione 3. Organizzazione 4. Conservazione 5. consultazione 6. Elaborazione 7. Selezione 8. Utilizzo 9. Comunicazione (su autorizzazione dell'amministratore) 10. Diffusione(su autorizzazione dell'amministratore)</p>
H)	Tutti gli autorizzati degli	DATI SENSIBILI	1) Raccolta

OPERATORE INSERIMENTO DATI	OSSERVATOR I Tutti gli autorizzati della DIREZIONE	DATI COMUNI	a) Diretta presso l'interessato; b) Utilizzo di archivi regionali; c) Acquisizione archivi da soggetti terzi (pubblici o privati). 2) Registrazione 3) Consultazione
I) UTENTE DI CONTROLLO	Membri Comitato di indirizzo e controllo Membri Collegio dei revisori dei Conti	DATI COMUNI DATI SENSIBILI	1) Consultazione

3. RESPONSABILE DELLA PROTEZIONE DEI DATI

3.1 Soggetti obbligati

Nel Regolamento viene introdotta la figura del Responsabile della protezione dei dati (RDP o DPO se si usa l'acronimo inglese).

Il soggetto suddetto è incaricato di assicurare una gestione corretta dei dati personali delle imprese e degli enti.

L'articolo 37 del Regolamento UE prevede:

1. Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta:

a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;

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

c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10.

2. Un gruppo imprenditoriale può nominare un unico responsabile della protezione dei dati, a condizione che un responsabile della protezione dei dati sia facilmente raggiungibile da ciascuno stabilimento.

3. Qualora il titolare del trattamento o il responsabile del trattamento sia un'autorità pubblica o un organismo pubblico, un unico responsabile della protezione dei dati può essere designato per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione.

4. Nei casi diversi da quelli di cui al paragrafo 1, il titolare e del trattamento, il responsabile del trattamento o le associazioni e gli altri organismi rappresentanti le categorie di titolari del trattamento o di responsabili del trattamento possono o, se previsto dal diritto dell'Unione o degli Stati membri, devono designare un responsabile della protezione dei dati. Il responsabile della protezione dei dati può agire per dette associazioni e altri organismi rappresentanti i titolari del trattamento o i responsabili del trattamento.

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

6. Il responsabile della protezione dei dati può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi.

7. Il titolare del trattamento o il responsabile del trattamento pubblica i dati di contatto del responsabile della protezione dei dati e li comunica all'autorità di controllo.”

Per chiarire meglio questi concetti intervengono le “Linee-guida sui responsabili della protezione dei dati (RPD)” e le relative FAQ. In particolare le stesse prevedono che *“Anche ove il regolamento non imponga in modo specifico la designazione di un RPD, può risultare utile procedere a tale designazione su base volontaria. Il Gruppo di lavoro “Articolo29” (Gruppo di lavoro) incoraggia gli approcci di questo genere. Ancor prima dell'adozione del RGPD, il Gruppo di lavoro ha sostenuto che questa figura rappresenti un elemento fondante ai fini della responsabilizzazione, e che la nomina del RPD possa facilitare l'osservanza della normativa e aumentare il margine competitivo delle imprese. Oltre a favorire l'osservanza attraverso strumenti di accountability (per esempio, supportando valutazioni di impatto e conducendo o supportando audit in materia di protezione dei*

dati), i RPD fungono da interfaccia fra i soggetti coinvolti: autorità di controllo, interessati, divisioni operative all'interno di un'azienda o di un ente.”

I DPO non rispondono personalmente in caso di inosservanza del Regolamento UE. Quest'ultimo chiarisce che spetta al titolare o al responsabile (esterno) del trattamento garantire ed essere in grado di dimostrare che le operazioni di trattamento siano conformi alle disposizioni del Regolamento UE (articolo 24, primo paragrafo). L'onere di assicurare il rispetto della normativa in materia di protezione dei dati ricade sul titolare o sui responsabili (esterni).

La nomina del DPO è solo il primo passo, perché lo stesso deve disporre anche di autonomia e risorse sufficienti a svolgere in modo efficace il compito cui è chiamato.

al titolare o al responsabile del trattamento spetta il compito fondamentale di consentire lo svolgimento efficace dei compiti cui il DPO è preposto.

Tranne quando sia evidente che un soggetto non è tenuto a nominare un DPO, il WP29 raccomanda ai titolari e responsabili di documentare le valutazioni compiute all'interno dell'azienda o dell'ente per stabilire se si applichi o meno l'obbligo di nomina di un RDP, così da poter dimostrare che l'analisi ha preso in esame correttamente i fattori pertinenti.

ARS deve procedere alla nomina obbligatoria del DPO in quanto rientra nei soggetti di cui all'art. 37, comma 1 lettera a) “*autorità pubblica o da un organismo pubblico*” .

Le principali attività del DPO sono indicate nello stesso art. 37, paragrafo 1, lettere b) e c) del Regolamento UE., che contiene un riferimento alle “*attività principali del titolare del trattamento o del responsabile del trattamento*”. Con l'espressione “attività principali” si possono intendere le operazioni che sono necessarie al raggiungimento degli obiettivi perseguiti dal titolare o dal responsabile del trattamento. Tuttavia la stessa non va interpretata nel senso di escludere quei casi in cui il trattamento costituisce una componente inscindibile delle attività svolte dal titolare o dal responsabile.

D'altra parte, tutti gli organismi (pubblici e privati) svolgono determinate attività quali ad esempio il pagamento delle retribuzioni del personale o dispongono di strutture standard di supporto informatico. Si tratta di funzioni di supporto necessarie ai fini dell'attività principale p dell'oggetto principale del singolo organismo, ma pur necessarie o perfino essenziali sono considerate solitamente di natura accessoria e non vengono annoverate fra le attività principali.

In base all'articolo 37, paragrafo 1, lettere b) e c) del regolamento, occorre che il trattamento dei dati personali avvenga su larga scala per far scattare l'obbligo di nomina del DPO. IL WP29 raccomanda di tener conto, in particolare, dei fattori elencati nel prosieguo al fine di stabilire se un trattamento sia effettuato su larga scala:

- il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;
- il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;
- durata, ovvero persistenza, dell'attività di trattamento;
- la portata geografica dell'attività di trattamento.

Alcuni esempi di trattamenti su larga scala sono i seguenti:

- trattamento di dati relativi a pazienti svolto da un ospedale nell'ambito delle proprie ordinarie attività;
- trattamento di dati relativi agli spostamenti di utenti di un servizio di trasporto pubblico cittadino (per esempio, il loro tracciamento attraverso titoli di viaggio);
- trattamento di dati relativi alla clientela da parte di una compagnia assicurativa o di una banca nell'ambito delle ordinarie attività.

Una delle principali attività del DPO è il monitoraggio regolare e sistematico.

Con questa espressione si intendono tutte le forme di tracciamento e profilazione su internet anche per finalità di pubblicità comportamentale.

Vale la pena evidenziare che anche qualora il titolare sia tenuto, in base ai criteri suddetti a nominare un DPO, il suo eventuale responsabile del trattamento non è detto sia ugualmente tenuto a procedere a tale nomina, che però può costituire una buona prassi. Quale buona prassi, il WP29 raccomanda che il DPO nominato da un soggetto responsabile del trattamento vigili anche sulle attività svolte da tale soggetto quando operi in qualità di autonomo titolare del trattamento.

3.2 Caratteristiche soggettive

Il DPO deve essere in grado di comunicare con gli interessati in modo efficiente e di collaborare con le autorità di controllo interessate. Ciò significa, fra l'altro, che le comunicazioni in questione devono avvenire nella lingua utilizzata dalle autorità di controllo e dagli interessati volta per volta in causa. Poiché il DPO è chiamato ad una molteplicità di funzioni, il titolare deve assicurarsi che un unico DPO sia in grado di adempiere in modo efficiente a tali funzioni anche se designato da una molteplicità di autorità e organismi pubblici.

Nel considerando 97 si prevede 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.

Il livello di conoscenza specialistica richiesto non trova una definizione tassativa; piuttosto, deve essere proporzionato alla sensibilità, complessità e quantità dei dati sottoposti a trattamento.

Per esempio, se il trattamento rivestisse particolare complessità oppure comportasse un volume consistente di dati sensibili, il DPO avrebbe probabilmente bisogno di un livello più elevato di conoscenze specialistiche e di supporto. Occorre anche distinguere in base all'esistenza di trasferimenti sistematici ovvero occasionali di dati personali al di fuori dell'Unione europea. Fra le competenze e le conoscenze specialistiche rientrano le seguenti:

- conoscenza della normativa e delle prassi nazionali ed europee in materia di protezione di dati, compresa un'approfondita conoscenza del Regolamento UE;
- familiarità con le operazioni di trattamento svolte;
- familiarità con le tecnologie informatiche e misure di sicurezza dei dati;
- conoscenza dello specifico settore di attività e dell'organizzazione del titolare/responsabile;
- capacità di promuovere la cultura della protezione dati all'interno dell'organizzazione del titolare/responsabile;
- nel caso di autorità pubblica o di un organismo pubblico, il DPO deve possedere anche una conoscenza approfondita delle norme e delle procedure amministrative applicabili;
- **capacità di assolvere i propri compiti:** con tale espressione si deve intendere sia quanto è legato alle qualità personali e alle conoscenze del DPO, sia quanto dipende dalla posizione del DPO all'interno dell'ente. Le qualità personali dovrebbero comprendere, per esempio, l'integrità ed elevati standard deontologici; il DPO dovrebbe perseguire in via primaria l'osservanza delle disposizioni del Regolamento. Il DPO infatti svolge un ruolo chiave nel promuovere la cultura della protezione dei dati all'interno dell'ente e contribuisce a dare attuazione a elementi essenziali del Regolamento stesso, quali principi fondamentali di ciascun trattamento,, la sicurezza degli stessi e la notifica e la comunicazione delle violazioni personali.

Il DPO può essere anche esterno all'ente. In questo caso le relative funzioni saranno esercitate in base ad un contratto di servizio stipulato con una persona fisica o giuridica. Se il DPO è esterno, si applicano tutti i requisiti fissati negli articoli 37 e 39.

Se la funzione di DPO è svolta da un fornitore esterno, i compiti stabiliti per il DPO potranno essere assolti efficacemente da un team operante sotto l'autorità di un contatto principale designato e responsabile per il singolo cliente.

In tal caso, è indispensabile che ciascun soggetto appartenente al fornitore esterno operante quale DPO soddisfi tutti i requisiti applicabili come fissati nel Regolamento, in particolare, è indispensabile che nessuno di tali soggetti versi in situazione di in conflitto di interessi.

Per favorire efficienza e correttezza, le linee-guida raccomandano di procedere a una chiara ripartizione dei compiti del team del DPO esterno, attraverso il contratto di servizio e di prevedere che sia un soggetto solo a fungere da contatto principale e incaricato per ciascun cliente.

I dati di contatto del DPO devono comprendere tutte le informazioni che consentono agli interessati e alle autorità di controllo di raggiungere facilmente il DPO stesso: recapito postale, numero telefonico, indirizzo dedicato di posta elettronica.

Se opportuno, per facilitare la comunicazione con il pubblico, si indicano anche canali ulteriori: una hotline dedicata, un modulo specifico per contattare il DPO pubblicato sul sito istituzionale nella pagina dedicata al DPO (<https://www.ars.toscana.it/responsabile-della-protezione-dei-dati-rdp-dpo.html>).

Sebbene non sia necessario pubblicare il nominativo del DPO, ARS ha ritenuto opportuno pubblicarlo, come buona prassi, ritenendo che si tratti di un'informazione necessaria nella specifica circostanza.

Inoltre seguendo quanto raccomandato dal WP29 ha provveduto a comunicare il nominativo e i relativi dati di contatto all'autorità di controllo e ai dipendenti.

Articolo 38 Posizione del responsabile della protezione dei dati

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

2. Il titolare e del trattamento e il responsabile del trattamento sostengono il responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'articolo 39 fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica.

3. Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti. Il responsabile della protezione dei dati non è rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti. Il responsabile della protezione dei dati riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento.

4 Gli interessati possono contattare il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento.

5. Il responsabile della protezione dei dati è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti, in conformità del diritto dell'Unione o degli Stati membri.

6. Il responsabile della protezione dei dati può svolgere altri compiti e funzioni. Il titolare del trattamento o il responsabile del trattamento si assicura che tali compiti e funzioni non diano adito a un conflitto di interessi.

Secondo l'articolo sopra riportato, è essenziale che il DPO sia coinvolto quanto prima possibile in ogni questione attinente la protezione dei dati. Per quanto concerne le valutazioni di impatto sulla protezione dei dati, Il regolamento prevede espressamente che il DPO sia coinvolto fin dalle fasi iniziali e specifica che il titolare abbia l'obbligo di consultarlo nell'effettuazione di queste valutazioni.

E' importante che il DPO sia annoverato tra gli interlocutori all'interno della struttura e che partecipi ai gruppi di lavoro che volta per volta si occupano delle attività di trattamento.

Occorre garantire:

- che il DPO sia invitato a partecipare su base regolare alle riunioni del management di alto e medio livello;
- la presenza del DPO ogni qualvolta debbano essere assunte decisioni che impattano sulla protezione dei dati. Il DPO deve disporre tempestivamente di tutte le informazioni pertinenti in modo da rendere una consulenza idonea;
- che il parere del DPO riceva sempre dovuta considerazione. In caso di disaccordi, il WP29 raccomanda, quale buona prassi, di documentare le motivazioni che hanno portato a condotte difformi da quelle raccomandate dal DPO;
- che il DPO sia consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente;

Il DPO deve poter contare sulle seguenti risorse:

- supporto attivo della funzione di DPO da parte dei senior management;
- tempo sufficiente per l'espletamento dei compiti affidati;
- supporto adeguato in termini di risorse finanziarie, infrastrutture (sede, attrezzature, strumentazione) e, ove opportuno, personale;
- comunicazione ufficiale della designazione del DPO a tutto il personale;
- accesso garantito ad altri servizi all'interno della struttura del titolare in modo da ricevere tutto il supporto, le informazioni o gli input necessari;
- formazione permanente.

In linea di principio, quanto più aumentano la complessità e/o sensibilità dei trattamenti, tanto maggiori devono essere le risorse messe a disposizione del DPO. La funzione "protezione dati" deve poter operare con efficienza e contare su risorse sufficienti in proporzione al trattamento svolto.

Un capitolo a parte è rappresentato dall'**indipendenza del DPO**.

Il DPO, nell'esercizio dei compiti attribuitigli ai sensi dell'art. 39, non deve ricevere istruzioni sull'approccio da seguire nel caso specifico – quali siano i risultati attesi, come condurre gli accertamenti su un reclamo, se consultare o meno l'autorità di controllo.

Né deve ricevere istruzioni sull'interpretazione da dare a una specifica questione attinente alla normativa in materia di protezione di dati.

Tuttavia l'autonomia non comporta che il DPO disponga di un margine decisionale superiore al perimetro dei compiti fissati dall'art. 39.

Il titolare mantiene la piena responsabilità dell'osservanza della normativa in materia di protezione di dati e deve essere in grado di dimostrare l'osservanza. Se il titolare assume una decisione incompatibile con il Regolamento e le indicazioni fornite dal DPO, quest'ultimo dovrebbe avere la possibilità di manifestare il proprio dissenso ai decisori.

Penalizzazioni. L'articolo 38, inoltre, prevede che il DPO "*non è rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti*". Il divieto di penalizzazioni si applica solo con riguardo a quelle eventualmente derivanti dall'esercizio del compito del DPO.

Le penalizzazioni posso assumere molte forme ed avere natura diretta o indiretta. Per esempio potrebbero consistere nella mancata o ritardata promozione nel blocco delle progressioni di carriera, nella mancata concessione di incentivi rispetto ad altri dipendenti. Non è necessario che si arrivi all'effettiva applicazione di una penalizzazione, essendo sufficiente anche la sola minaccia nella misura in cui sia rivolta al DPO in rapporto alle attività da questi svolte.

Viceversa è legittimamente possibile interrompere il rapporto con il DPO per motivazioni diverse dallo svolgimento dei compiti che gli sono propri.

Conflitto di interessi. L'assenza di conflitto di interessi è strettamente connessa agli obblighi di indipendenza. Anche se un DPO può svolgere altre funzioni, l'affidamento di tali ulteriori compiti e funzioni è possibile solo a condizione che essi non diano adito a conflitti di interessi, Ciò significa, in modo particolare, che un DPO non può rivestire, all'interno dell'organizzazione del titolare o del responsabile, un ruolo che comporti la definizione delle finalità o modalità del trattamento di dati personali (sono sconsigliati DPO appartenenti alle aree del personale e dei sistemi informativi). Al riguardo, si deve ricordare, inoltre, che un conflitto di interessi può assumere varie configurazioni a seconda che il DPO sia designato fra soggetti interni o esterni all'organizzazione.

Articolo 39 Compiti del responsabile della protezione dei dati

1. Il responsabile della protezione dei dati è incaricato almeno dei seguenti compiti:

a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

b) sorvegliare l'osservanza del presente 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, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;

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

d) cooperare con l'autorità di controllo; e

e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

2. Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

Il ruolo del DPO nella valutazione di impatto sulla protezione dei dati (DPIA, nell'acronimo inglese) è descritto dal WP29, che raccomanda che il titolare si consulti con il DPO, fra l'altro sulle seguenti tematiche:

- se condurre o meno una DPIA;
- quale metodologia adottare nel condurre una DPIA;
- se condurre la DPIA con risorse interne o esternalizzare;
- quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi per i diritti e gli interessi delle persone interessate;

- se la DPIA sia stata condotta correttamente o meno, e se le conclusioni raggiunte (procedere o meno con il trattamento e quali salvaguardie applicare) siano conformi al RGPD.

Qualora il titolare non concordi con le indicazioni fornite dal DPO, è necessario che la documentazione relativa alla DPIA riporti specificatamente per iscritto le motivazioni per cui si è ritenuto di non conformarsi a tali indicazioni.

Circa la tenuta del **registro delle attività di trattamento**, occorre fare una precisazione.

L'articolo 30 prevede che sia il titolare o il responsabile del trattamento e non il DPO a tenere il registro delle attività di trattamento. Nella realtà sono spesso i DPO a realizzare l'inventario dei trattamenti e a tenere il registro.

L'articolo 39, primo paragrafo, contiene un elenco non esaustivo dei compiti affidati al DPO, pertanto niente vieta di affidare allo stesso il compito di tenere il registro delle attività di trattamento sotto la responsabilità del titolare stesso. Tale registro va considerato uno degli strumenti che consentono al DPO di adempiere agli obblighi di sorveglianza del rispetto del Regolamento, informazione e consulenza nei riguardi del titolare.

In ogni caso, il registro la cui tenuta è obbligatoria ai sensi dell'articolo 30 deve essere considerato anche uno strumento che consenta al titolare e all'autorità di controllo, su richiesta, di svolgere di disporre un quadro complessivo dei trattamenti dei dati personali svolti dallo specifico soggetti. In quanto tale, esso costituisce un presupposto indispensabile ai fini dell'osservanza delle norme e, pertanto, un'efficace misura di responsabilizzazione.

3.4 Ufficio del DPO

Il titolare del trattamento è tenuto a fornire al RPD le risorse - economiche, strutturali ed organizzative - per assolvere i suoi compiti.

Ne è derivato che, in relazione alla complessità (amministrativa e tecnologica) dei trattamenti e dell'organizzazione, è stato valutato necessario istituire un apposito ufficio al quale destinare le risorse necessarie allo svolgimento dei compiti stabiliti un ufficio DPO.

L'ufficio è costituito da professionalità interne all'Agenzia che hanno rilevanza interna come soggetti portatori presso il DPO delle istanze provenienti dalle strutture dell'Agenzia e curano gli adempimenti previsti dal GDPR, ma anche esterna in quanto sono riconosciuti come referenti dell'ente di fronte al DPO.

E' infatti necessaria un'approfondita attività di monitoraggio iniziale (sulle attività svolte nelle varie strutture interessate) ai fini del censimento dei trattamenti effettuati dall'ARS, che richiedono necessariamente il coinvolgimento di più soggetti, con competenze e formazione diversificati. Senza pensare che le misure sicurezza richiedono un aggiornamento, e che l'applicazione della normativa sulla privacy deve essere continuamente monitorata.

All'ufficio DPO sono, altresì, attribuiti compiti di monitoraggio con specifico riguardo alle tipologie di banche dati detenute, sia elettroniche sia cartacee, agli strumenti elettronici utilizzati per il trattamento (elaboratori stand-alone, computer collegati in rete locale, connessione a rete aperta ecc.), ai flussi informativi verso l'esterno e quelli infra-strutture e all'ambito di comunicazione e di diffusione dei dati.

I dati così raccolti saranno utilizzati dall'ufficio DPO per predisporre la modulistica necessaria (comunicazione, informativa, aggiornamento misure di sicurezza, predisposizione atto di natura regolamentare (ove necessario) e per adempiere agli altri obblighi previsti dalla normativa e dalle presente prescrizioni.

Oltre all'attività di monitoraggio i membri dell'ufficio concorrono con i delegati, anche alle attività di controllo interno, verificando la corrispondenza e la correttezza delle attività esercitate rispetto a quanto previsto in sede normativa.

L'ufficio DPO è un organismo permanente.

Il Titolare ha provveduto ad individuare due specifiche professionalità: una giuridica e una informatica. Tale ufficio può essere esteso a seconda della materia trattata anche a soggetti diversi (ad esempio statistici, quando siano necessarie competenze tecniche specifiche).

I compiti dell'ufficio DPO sono di seguito meglio specificati:

- individua le misure più adeguate ed efficaci per la tutela della riservatezza, integrità e disponibilità del patrimonio informativo di ARS. Tutte le soluzioni che abbiano un significativo impatto sulla protezione dei dati personali sono sottoposte a parere preventivo obbligatorio del DPO, come ad esempio per la redazione delle linee guida in materia di sicurezza delle informazioni e protezione dei dati personali e per la redazione ed aggiornamento dei disciplinari tecnici trasversali;
- condivide le evidenze dell'analisi dei rischi con il responsabile dei sistemi informativi, il quale fornisce parere obbligatorio sulle misure poste a mitigazione del rischio che abbiano un significativo impatto sulla protezione dei dati personali;
- provvede, ogni qualvolta venga avvertito un problema di sicurezza a: ○ attivare la struttura cui sono demandati compiti relativi alla gestione degli incidenti di sicurezza, assicurando la partecipazione del DPO;
- individua misure idonee al miglioramento della sicurezza dei trattamenti dei dati personali, previo parere obbligatorio del DPO;
- segnala al Titolare le violazioni dei dati personali ai fini della notifica, ai sensi dell'art. 33 del Regolamento, al Garante per la protezione dei dati personali;
- svolge verifiche sulla puntuale osservanza della normativa delle policy aziendali in materia di sicurezza delle informazioni e di trattamento di dati personali, prevedendo la partecipazione del DPO e realizza le verifiche specifiche richieste dello stesso;
- promuove la formazione di tutto il personale di ARS in materia di protezione dei dati e sicurezza informatica, , coordinandosi con le azioni promosse dal DPO.
- funge da anello di congiunzione fra il DPO e le strutture dell'Agenzia;
- pone tutti gli adempimenti giuridici necessari per rendere l'organizzazione di ARS in compliance con il GDPR.

3.5 Pareri del DPO

Attraverso l'ufficio DPO istituito presso ARS, di cui al paragrafo precedente, è possibile ottenere l'espressione di pareri da parte del DPO.

Il DPO fornisce il proprio parere in ordine alla legittimità e alla correttezza dei trattamenti di dati personali sulle istanze che le strutture di ARS presentano nei seguenti casi:

Pareri obbligatori nei casi di seguito indicati

Devono essere obbligatoriamente richiesti pareri in ordine a:

- individuazione delle misure che abbiano un significativo impatto sulla protezione dei dati personali che ARS tende adottare ai fini della tutela della riservatezza, integrità e disponibilità del patrimonio informativo di ARS anche a seguito di incidenti di sicurezza o analisi dei rischi;
- adozione di policy e disciplinari in materia di protezione dei dati personali e sicurezza delle informazioni, redazione e aggiornamento dei disciplinari tecnici con impatto sulla sicurezza delle informazioni;

- individuazione di misure poste a mitigazione del rischio delle criticità emerse dall'analisi dei rischi, che abbiano un significativo impatto sulla protezione dei dati personali;
- incidenti sicurezza.

Pareri facoltativi .

Possono essere inoltre richiesti, se ritenuti utili, pareri in ordine a:

- progettazione di nuove applicazioni
- modifica sostanziale di quelle esistenti, in aderenza al principio della privacy by design e by default;
- valutazione d'impatto sulla protezione dei dati ai sensi dell'articolo 35 del Regolamento 2016/679;
- valutazione dell'eventuale pregiudizio che l'accesso civico potrebbe comportare agli interessi dei controinteressati, nella misura in cui questi afferiscono alle tutele dei loro dati personali ai sensi del comma 2 dell'art. 5-bis e, in via generale, del Regolamento UE n. 679/2016;
- opposizione formulata dai controinteressati nella misura in cui questa sia riferibile ad elementi afferenti alla protezione dei dati personali, valutando la probabilità e la serietà del danno agli interessi degli oppositori. Le richieste di parere devono essere inviate all'indirizzo di posta elettronica dpo@ars.toscana o presentare le richieste di parere i soggetti delegati o i Responsabili delegati.

I pareri sono espressi con la seguente modalità:

- “non conformità”, nei casi in cui siano rilevati elementi di non conformità alla normativa e alle policy in materia di protezione dei dati personali;
- “osservazione”, nei casi in cui vi siano elementi di miglioramento che garantiscono una maggiore aderenza alla normativa e alle policy in materia di protezione dei dati personali, non costituendo vincolo di attuazione;
- “positivo”, nei casi in cui siano prospettati elementi valutati come conformi alla normativa e alle policy regionali in materia di protezione dei dati personali. Nei casi in cui il DPO esprima pareri “non conforme” e “osservazione” il soggetto delegato o i responsabili delegati devono formalizzare, nelle medesime forme utilizzate dal DPO per l'espressione del parere, le motivazioni che giustificano l'esecuzione dell'attività o l'implementazione della soluzione tecnologica, in contrasto alle indicazioni fornite dal DPO. I pareri espressi dal DPO sono conservati agli atti dell'ufficio DPO presso ARS.

3.6 Accesso civico generalizzato e ruolo DPO

Con specifico riferimento alla normativa in materia di trasparenza, si ritiene opportuno disciplinare la necessaria interazione tra il DPO, le strutture di ARS, e il Responsabile per la prevenzione della corruzione e trasparenza (R.P.C.T.). Il D.L. n. 97/2016, di modifica del D.lgs. 33/2013 ha introdotto l'istituto dell'accesso civico “generalizzato”, che attribuisce a “chiunque” il “diritto di accedere ai dati e ai documenti detenuti dalle pubbliche amministrazioni, ulteriori rispetto a quelli oggetto di pubblicazione. L'esercizio di tale diritto soggiace ai limiti relativi alla tutela di interessi giuridicamente rilevanti secondo quanto previsto dall'articolo 5-bis” del d.lgs. n. 33/2013. L'art. 5, comma 5, d.lgs. n. 33/2013 prevede che, per ciascuna domanda di accesso generalizzato, l'amministrazione debba verificare l'eventuale esistenza di controinteressati, eccetto i casi in cui la richiesta di accesso civico abbia ad oggetto dati la cui pubblicazione è prevista dalla legge come obbligatoria. In attuazione di quanto normativamente previsto, ARS ha adottato e pubblicato sul proprio sito istituzionale un'apposita sezione dedicata all'accesso civico e generalizzato, nel quale sono indicate le modalità di esercizio del diritto di accesso.

Il DPO funge da supporto alle strutture competenti sulle singole richieste di accesso nella fase di individuazione dei soggetti da ritenersi controinteressati e comunque per tutti gli aspetti relativi alla protezione dei dati personali inerenti le richieste di accesso civico generalizzato.

Il DPO funge altresì da supporto al R.P.C.T. nei casi di riesame di istanze di accesso negato o differito a tutela dell'interesse alla protezione dei dati personali. Il DPO, inoltre, su richiesta delle strutture, esprime proprio parere in ordine alla valutazione dell'eventuale pregiudizio che l'accesso potrebbe comportare agli interessi dei controinteressati, nella misura in cui questi afferiscono alle tutele dei loro dati personali ai sensi del comma 2 dell'art. 5-bis e, in via generale, del Regolamento UE n. 679/2016.

Il DPO, su richiesta delle strutture, formula il proprio parere, entro tre giorni, in ordine all'opposizione formulata dai controinteressati nella misura in cui questa sia riferibile ad elementi afferenti alla protezione dei dati personali, valutando la probabilità e la serietà del danno agli interessi degli oppositori. Sulla scorta di tale parere le strutture competenti sulle singole richieste di accesso effettueranno il bilanciamento tra gli interessi asseritamente lesi e la rilevanza dell'interesse conoscitivo della collettività che la richiesta di accesso mira a soddisfare.

4. ADEMPIMENTI VERSO GLI INTERESSATI

L'art 12 del Reg. (ue) n. 679/2016, enuncia il principio di trasparenza.

Con tale principio, il Regolamento pone al centro dell'attività compiuta dai soggetti che svolgono il trattamento dei dati, l'accessibilità ad essa da parte dell'interessato, intesa come conoscibilità da parte del soggetto, del suo diritto all'esercizio del controllo sui dati che lo riguardano e degli effetti che i trattamenti possono avere. Tale principio, trova manifestazione sia nelle informazioni obbligatorie di cui agli artt. 13 e 14, che nel riscontro alle richieste presentate ai sensi degli artt. dal 15 al 22.

Il principio di trasparenza, non si limita a un dovere informativo sul trattamento dei dati, esso riguarda anche l'informazione circa le modalità con cui, colui che pone in essere l'attività di trattamento, sia esso Titolare o Responsabile, deve fornire le informazioni al soggetto interessato.

La trasparenza costituisce un elemento indispensabile del trattamento, insieme alla liceità e alla correttezza. La trasparenza è infatti un principio fondamentale del trattamento, oltre che un vero e proprio diritto dell'interessato.

Il principio in questione non riguarda solo i trattamenti, ma è alla base dei rapporti tra il titolare e l'interessato. In tal senso, le informative e le comunicazioni verso l'interessato e quindi l'informativa in particolare, devono essere facilmente accessibili e comprensibili con particolare attenzione quando l'informazione è rivolta ai minori. Devono pertanto essere scritte utilizzando un linguaggio semplice, eventualmente anche tramite grafica e icone, qualora siano forniti in forma elettronica, in modo che gli interessati siano in grado di capirne il contenuto e comprendere come sono trattati i loro dati. L'interessato come sopra evidenziato deve essere in grado di apprezzare anche i rischi che i trattamenti possono comportare, com'è ad esempio nel caso di trattamenti di dati che comprendono flussi transfrontalieri (extra-UE) di dati personali. In tal modo senso anche la valutazione di rischio diventa oggetto dell'obbligo di trasparenza, ed è doveroso che sia svolta e che l'esito sia reso noto sia nei confronti degli interessati che, qualora il trattamento comporti un rischio elevato, all'Autorità di controllo.

Qualsiasi trattamento occulto o segreto deve, quindi, ritenersi illecito. I titolari e i responsabili devono garantire agli interessati che i dati saranno trattati secondo liceità e correttezza. L'obbligo di

garantire la trasparenza dei trattamenti grava anche sul Responsabile, ed il Titolare è tenuto a verificare l'adeguamento del Responsabile al principio sopra enunciato, prima di designarne uno.

4.1 L'informativa

Il principio di trasparenza impone al titolare del trattamento l'adozione di misure appropriate, sia tecniche sia organizzative, per fornire agli interessati tutte quelle informazioni, previste dagli articoli 13 e 14 del regolamento, che spieghino agli interessati le finalità specifiche per le quali sono stati raccolti i loro dati, quali sono le norme, le garanzie e le modalità del trattamento, a quali rischi potrebbero essere esposti, quali sono i loro diritti (articoli 15-22 regolamento, ove applicabili) e come esercitarli.

Di tale obbligo, il titolare può essere chiamato in qualunque momento a renderne conto.

I contenuti dell'informativa sono elencati in modo tassativo negli articoli 13, paragrafo 1, e 14, paragrafo 1, del Regolamento. In particolare, il titolare deve sempre specificare:

e) i propri dati di contatto e quelli del DPO (Data Protection Officer, figura obbligatoria per i soggetti pubblici); le finalità del trattamento e la base giuridica del trattamento; qualora il trattamento si basi sui legittimi interessi di cui all'art. 6, lett. f), l'indicazione di essi se non è effettuato dall'autorità pubblica nell'esercizio dei suoi compiti; i destinatari o le categorie di destinatari dei dati personali; nonché se trasferisce i dati personali in Paesi terzi o a organizzazioni internazionali, se vi è una decisione di adeguatezza della Commissione o, nel caso di trasferimenti per cui ci sia necessità di adottare mezzi di tutela particolari (art. 46; 47 o 49, 2 comma) attraverso quali strumenti l'indicazione delle garanzie appropriate o opportune e dei mezzi con cui il soggetto può richiedere una copia dei dati nel luogo in cui sono stati resi disponibili. (esempio: si tratta di un Paese terzo giudicato adeguato dalla Commissione europea; si utilizzano BCR di gruppo; sono state inserite specifiche clausole contrattuali modello, ecc.). Inoltre, nel caso di trattamenti di dati personali raccolti presso una fonte diversa dall'interessato (ad es. da altra pubblica amministrazione), applicandosi dunque il disposto ex art. 14 GDPR, andrà specificata la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico (art. 14, comma 2, lett. F).

Il regolamento prevede anche ulteriori informazioni che devono essere fornite all'interessato, in quanto "necessarie per garantire un trattamento corretto e trasparente". Il titolare deve specificare il periodo di conservazione dei dati o, qualora non possa essere definito, i criteri seguiti per stabilire tale periodo di conservazione e il diritto di presentare un reclamo all'autorità di controllo. Se il trattamento comporta processi decisionali automatizzati (quali la profilazione), l'informativa deve specificarlo e deve indicare anche la logica di tali processi decisionali e le conseguenze previste per l'interessato.

L'informativa deve essere data agli interessati sempre prima di iniziare il trattamento.

Nel caso in cui i dati personali non siano raccolti direttamente presso l'interessato (*art. 14 del regolamento*), l'informativa deve essere fornita entro un termine ragionevole e non oltre può superare 1 mese dalla raccolta dei dati, oppure al momento della comunicazione dei dati a terzi o all'interessato.

Il regolamento fissa i requisiti presupposti per l'esonero dalla informativa: spetta al titolare, in caso di dati personali raccolti da fonti diverse dall'interessato, valutare se la prestazione dell'informativa agli interessati risulti impossibile o comporti uno sforzo sproporzionato.

L'informativa deve avere forma concisa, trasparente, intelligibile per l'interessato e deve essere facilmente accessibile; occorre utilizzare un linguaggio chiaro e semplice, e per i minori occorre prevedere informative idonee, scritte in una forma e con un linguaggio comprensibile dagli stessi.

L'informativa è data, in linea di principio, per iscritto e preferibilmente in formato elettronico, soprattutto nel contesto di servizi online, anche se sono ammessi "altri mezzi", quindi può essere fornita anche oralmente, ma solo se lo richiede l'interessato stesso.

Il regolamento ammette l'utilizzo di icone per presentare i contenuti dell'informativa in forma sintetica, ma solo "in combinazione" con l'informativa estesa; queste icone dovranno essere identiche in tutta l'Ue e saranno definite prossimamente dalla Commissione europea.

Modelli di informative per le strutture di ARS sono state inoltrate dall'ufficio DPO di ARS, via email.

I modelli contengono le informazioni minime obbligatorie previste dal regolamento, devono essere adattati al caso concreto e completati con le informazioni mancanti, possono essere integrate con contenuti ulteriori, ma i contenuti già previsti nei modelli non possono essere ridotti. (ALLEGATI DA N. 5 A N. 14).

Il Titolare ha provveduto a verificare la rispondenza dell'informativa utilizzata fino a maggio 2018 a tutti i criteri sopra delineati, con particolare riguardo ai contenuti obbligatori e alle modalità di redazione, e ha provveduto a dare mandato all'ufficio DPO di apportare le modifiche e le integrazioni necessarie a renderle legittime ai sensi del Regolamento UE.

4.2 La raccolta del consenso

Il consenso è una delle basi giuridiche del trattamento, nell'ambito del regolamento generale per la protezione dei dati personali.

E' importante tenere presente che il consenso è solo una delle sei basi giuridiche previste dal GDPR, ed è specifico dovere del titolare del trattamento valutare quale tra esse è la base giuridica più idonea per il trattamento che intende porre in essere. Chiedere il consenso dovrebbe essere ritenuta una richiesta insolita, spesso indica che il titolare vuole sottoporre i dati personali dell'interessato ad un trattamento che l'interessato potrebbe non gradire oppure non essere in grado di aspettarsi ragionevolmente. Il consenso era centrale con la vecchia normativa che instaurava una relazione tra titolare ed interessato, per cui c'era una visione proprietaria del dato, e occorreva il consenso per poterlo trattare. Oggi non è più così, considerato che un cittadino è costantemente soggetto a numerosi trattamenti per cui la tutela della circolazione del dato è essenziale come la tutela dello stesso dato.

Anche perché a seconda della base giuridica variano i diritti dell'interessato.

DEFINIZIONE

Il consenso, in base al nuovo Regolamento Generale (art. 4 GDPR), è qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso esprime il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, al trattamento dei dati personali che lo riguardano. Il presupposto indefettibile è che il soggetto che conferisce il consenso abbia la capacità giuridica per farlo.

Inoltre, in base al Considerando 32: "...il consenso dovrebbe essere espresso mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale. Ciò potrebbe comprendere la selezione di un'apposita casella in un sito web, la scelta di impostazioni tecniche per servizi della società dell'informazione o qualsiasi altra dichiarazione o qualsiasi altro comportamento che indichi chiaramente in tale contesto che l'interessato accetta il trattamento proposto. Non dovrebbe pertanto configurare consenso il silenzio, l'inattività o la preselezione di caselle. Il consenso dovrebbe applicarsi a tutte le attività di trattamento svolte per la stessa o le stesse finalità. Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste. Se il consenso dell'interessato è richiesto attraverso mezzi elettronici, la richiesta deve essere chiara, concisa e non interferire immotivatamente con il servizio per il quale il consenso è espresso".

CARATTERISTICHE

Se il titolare decide di basare il trattamento sul consenso deve assicurarsi che esso presenti le seguenti caratteristiche:

- 1) inequivocabile;
- 2) libero;
- 3) specifico;
- 4) informato;
- 5) verificabile;
- 6) revocabile.

1) Consenso inequivocabile (unambiguous nella versione inglese) vuol dire che non è necessario che sia esplicito ma può anche essere implicito (ma non tacito), purché, nel momento in cui sia desunto dalle circostanze, non sussista alcun dubbio che col proprio comportamento l'interessato abbia voluto comunicare il proprio consenso (es. l'inerzia non può costituire manifestazione di consenso, come anche i form precompilati e caselle già prespuntate). Ciò deve prevedere una chiara azione positiva (come spuntare una casella od inserire la mail in un campo dove è specificata la finalità per la quale sarà usato il dato).

Il consenso deve, invece, essere esplicito (art. 9 GDPR) nel caso di trattamento di dati sensibili o nel caso di processi decisionali automatizzati (es. profilazione).

Occorre dire che la versione originaria della proposta della Commissione europea prevedeva sempre il consenso esplicito, poi si è pervenuti al compromesso attuale.

2) Il consenso deve essere dato liberamente, il che significa che l'interessato deve essere in grado di operare una scelta effettiva, senza subire intimidazioni o raggiri, né deve subire conseguenze negative a seguito del mancato conferimento del consenso. L'articolo 7 del GDPR chiarisce che “nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto”.

Ad esempio, nel caso di progetto di ricerca in materia sanitaria, il consenso deve essere separato rispetto al consenso per la adesione/partecipazione al progetto richiesta all'utente, perché l'utente deve avere la possibilità di ricevere la prestazione senza dover subire il ricatto di non ricevere cure adeguate. Non può definirsi libero il consenso a ulteriori trattamenti dei dati personali che l'interessato debba prestare quale condizione per conseguire una prestazione richiesta (provvedimento del Garante del 31 gennaio 2008).

Questo purtroppo porta al rischio che molti dei consensi ottenuti dai servizi online possano essere ritenuti invalidi. Lo stesso Gruppo Articolo 29 fornisce un esempio chiarificatore: una app mobile per il fotoritocco chiede il consenso per accedere alla geolocalizzazione e i dati vengono utilizzati a fini di pubblicità comportamentale. Ma né la geolocalizzazione, né la pubblicità sono necessari per la fornitura del servizio (fotoritocco), per cui subordinare l'uso della App a tale consenso rende il consenso non libero e quindi illecito.

Un altro problema riguarda il consenso dei dipendenti. Se il datore di lavoro richiede il consenso all'utilizzo del dato (es. vuole pubblicare la foto dei dipendenti sul sito web aziendale) e vi è un pregiudizio reale o potenziale per il cliente non consenziente (cosa altamente probabile in un contesto lavorativo), il consenso non può ritenersi valido perché non libero. Dato lo squilibrio di potere tra datore e dipendente, quest'ultimo può dare un consenso valido solo in circostanze eccezionali. Quindi, il consenso non può costituire la base giuridica del trattamento in caso di evidente squilibrio tra le parti. In tal caso sarebbe preferibile trattare i dati su base giuridica differente.

3) Il consenso deve essere specifico, cioè relativo alla finalità per la quale è eseguito quel trattamento (granularità del consenso). Qualora il trattamento abbia più finalità, il consenso

dovrebbe essere prestato per ogni finalità (Considerando 32 GDPR). Quindi, i dati dovranno essere pertinenti al consenso fornito, e in caso di modifiche del trattamento occorre richiedere un nuovo consenso. Per cui avremo un consenso per la partecipazione al progetto diretto, un consenso per la profilazione, uno per il follow up...

4) Il consenso deve essere informato, occorre cioè che l'interessato sia posto in condizioni di conoscere quali dati sono trattati, con che modalità e finalità e i diritti che gli sono attribuiti dalla legge, cioè deve essere rispettato il principio di trasparenza. Inoltre l'interessato deve essere opportunamente informato sulle conseguenze del suo consenso (ad esempio deve essere indicato che in assenza di consenso non potrà accedere a determinate sezioni del sito web). L'informazione si ha attraverso l'apposita informativa, che in questo caso diventa una vera e propria condizione di legittimità del trattamento. Il regolamento europeo si concreta, più che sui requisiti formali del consenso, sulla necessità della validità sostanziale del consenso, per cui l'aspetto informativo è essenziale, richiedendo un linguaggio semplice e comprensibile, anche eventualmente colloquiale.

5) Consenso verificabile non vuol dire che il consenso deve essere documentato per iscritto, né che è richiesta la forma scritta (anche se in alcune ipotesi -es. dati sensibili- può essere preferibile perché consente più facilmente di provare il consenso, facilitando quindi le verifiche da parte dell'autorità), ma che l'ente deve essere in grado di dimostrare che l'interessato lo ha conferito con riferimento a quello specifico trattamento (quindi distinguendo tra i vari trattamenti). L'ente dovrà essere in grado di sapere anche a quale informativa l'utente ha acconsentito, distinguendo tra le varie versioni.

Il WP29 suggerisce di utilizzare un registro nel quale siano conservate le informazioni relative alla sessione in cui è stato espresso il consenso, unitamente alla documentazione del flusso di lavoro del consenso, e una copia delle informazioni presentate all'interessato in quel momento.

6) Il consenso deve essere revocabile in qualsiasi momento. La revoca deve essere facile così come lo è dare il consenso. Non vi è alcun obbligo di motivare la revoca, a seguito della quale il trattamento deve interrompersi (ovviamente la revoca non comporta illiceità del trattamento precedente, ma solo l'obbligo di terminare il trattamento), a meno che non sussista una differente base giuridica per continuare il trattamento.

Per revocare il consenso, quindi, il titolare dovrebbe predisporre una procedura analoga a quella offerta per concedere il consenso. In alternativa è possibile revocare il consenso inviando una comunicazione, o tramite un apposito form sul sito, o tramite mail, ai contatti indicati nel sito all'interno dell'informativa (interpello al titolare). Nel caso in cui il titolare non ottemperi, ci si può rivolgere al Garante o al tribunale per la tutela dei propri diritti.

Con la revoca si innesca il diritto di cancellazione, per cui l'ente deve cancellare i dati dell'utente. Ovviamente vi sono motivi legittimi in base ai quali un'azienda ha necessità di conservare alcuni dati dell'utente anche dopo la revoca del consenso, come ad esempio mantenere un registro delle transazioni per motivi fiscali. In ogni caso l'azienda può avvertire l'interessato che a seguito della revoca del consenso, vi sarà la cancellazione dei dati e la conseguente impossibilità di fornire ulteriori servizi.

SCADENZA

Occorre tenere presente che il consenso non dura per sempre. Quando si raccolgono dati personali occorre informare l'interessato della durata della conservazione (e quindi trattamento) del dato, scaduta la quale il dato va o anonimizzato oppure cancellato. Per questo motivo in alcuni casi potrebbe essere preferibile una base giuridica diversa dal consenso, come ad esempio i legittimi interessi del titolare del trattamento.

DATI SOGGETTI A TRATTAMENTO SPECIALE

Per i dati soggetti a trattamento speciale, cioè quelli che una volta si definivano dati sensibili, con in più i dati biometrici e genetici, sussiste un generale divieto di trattamento, con una serie di

esenzioni, tra i quali il consenso esplicito. A parte, ovviamente, il trattamento per l'attività giornalistica, che è a forma libera per qualsiasi tipo di dato.

MINORI

Il consenso dei minori è valido a partire dai 16 anni di età. Prima dei 16 anni occorre raccogliere il consenso dei genitori o di chi ne fa le veci.

PORTABILITÀ DEI DATI

Se il trattamento dei dati è basato sul consenso dell'interessato, questi acquisisce l'ulteriore diritto alla portabilità dei dati.

CONSENSO E REGOLAMENTO ePRIVACY

Il consenso è un prerequisito del regolamento ePrivacy. Quest'ultimo, infatti, nel disciplinare le comunicazioni elettroniche, compreso i cookie, fa riferimento alla definizione di consenso contenuta nella normativa generale, che oggi è il regolamento europeo. Di conseguenza nell'applicare la ePrivacy occorre sempre fare riferimento al consenso di cui al GDPR. Ad esempio, nella gestione dei cookie occorre che il consenso sia specifico, cioè separato per finalità.

4.3 I riscontro nell'esercizio dei diritti

Le modalità per l'esercizio di tutti i diritti da parte degli interessati sono stabilite in via generale dagli articoli 11 e 12 del Regolamento.

Il termine per la risposta all'interessato è, per tutti i diritti (compreso il diritto di accesso), un mese, estendibile fino a tre mesi in casi di particolare complessità; il titolare deve comunque dare un riscontro all'interessato entro un mese dalla richiesta, anche in caso di diniego. Spetta al titolare valutare la complessità del riscontro all'interessato e stabilire l'ammontare dell'eventuale contributo da chiedere all'interessato, ma solo se si tratta di richieste manifestamente infondate o eccessive (anche ripetitive) (articolo 12, paragrafo 5) a differenza di quanto prevedono gli articoli 9, comma 5, 10, commi 7 e 8, del Codice privacy ovvero se sono chieste più copie dei dati personali nel caso del diritto di accesso (articolo 15, paragrafo 3); in quest'ultimo caso il titolare deve tener conto dei costi amministrativi sostenuti. Il riscontro all'interessato deve avvenire di regola in forma scritta anche attraverso strumenti elettronici che ne favoriscano l'accessibilità; può essere dato oralmente solo se richiesto specificatamente dall'interessato (articolo 12, paragrafo 1, articolo 15, paragrafo 3). La risposta fornita all'interessato non solo deve essere intellegibile, ma anche concisa, trasparente e facilmente accessibile, oltre a utilizzare un linguaggio semplice e chiaro.

Mentre è rimasta pressoché invariata la precedente disciplina per quanto riguarda quanto di seguito descritto.

In particolare, il titolare del trattamento deve agevolare l'esercizio dei diritti da parte dell'interessato, adottando ogni misura tecnica e organizzativa a ciò idonea. Benché sia il solo titolare a dover dare riscontro in caso di esercizio dei diritti (articoli 15 -22), il responsabile è tenuto a collaborare con il titolare ai fini dell'esercizio dei diritti degli interessati (articolo 28 paragrafo 3, lettera e)).

L'esercizio dei diritti è, in linea di principio, gratuito per l'interessato, ma possono esservi eccezioni, come sopra spiegato.

Il titolare ha diritto a richiedere informazioni necessarie ad identificare l'interessato e quest'ultimo ha il dovere di fornirle secondo modalità idonee (articolo 11, paragrafo 2, articolo 12 paragrafo 6). Sono ammesse deroghe ai diritti riconosciuti dal regolamento, ma solo sul fondamento di disposizioni normative nazionali, ai sensi dell'articolo 23, nonché degli altri articoli relativi ad ambiti specifici (articolo 17, paragrafo 3 – diritto alla cancellazione e all'oblio- Articolo 83 – trattamento di natura giornalistica- e articolo 89 – trattamenti per finalità di ricerca scientifica o storica o statistica).

In questo senso, in via generale, possono continuare ad essere applicate tutte le deroghe previste dall'articolo 8, comma 2, del Codice privacy, in quanto compatibili con le disposizioni citate.

E' opportuno che il titolare adotti tutte le misure tecniche e organizzative eventualmente necessarie per favorire l'esercizio dei diritti ed il riscontro delle richieste presentate dagli interessati, che – a differenza di prima- dovrà avere forma scritta (anche elettronica).

I DIRITTI

Diritto di accesso- Articolo 15

Il diritto di accesso prevede in ogni caso il diritto di ricevere una copia dei personali oggetto del trattamento. Fra le informazioni che il titolare deve fornire non rientrano le “modalità” del trattamento, mentre occorre indicare il periodo di conservazione previsto o, se possibile, i criteri utilizzati per definire tale periodo, nonché le garanzie applicate in caso di trasferimento dei dati verso Paesi terzi.

Oltre al rispetto delle prescrizioni relative alla modalità di esercizio e degli altri diritti i titolari possono consentire agli interessati di consultare direttamente, da remoto, i propri dati personali (si veda considerando 68).

Diritto di cancellazione (diritto di oblio) – Articolo 17

Il diritto cosiddetto “all’oblio” si configura come un diritto alla cancellazione dei propri dati personali in forma rafforzata. Si prevede, infatti, l’obbligo per i titolari (se hanno “reso pubblici” i dati personali dell’interessato, ad esempio pubblicandoli su un sito web) di informare della richiesta di cancellazione altri titolari che trattano i dati personali cancellati, compresi “qualsiasi link, copia o riproduzione” (si veda articolo, 17, paragrafo 2).

Ha un campo di applicazione più esteso di quello che era previsto dall’articolo 7, comma 3, lettera b) del Codice privacy, poiché l’interessato ha il diritto di chiedere la cancellazione dei propri dati, per esempio anche dopo la revoca del consenso al trattamento (articolo 17, paragrafo 1).

Diritto alla limitazione del trattamento - Articolo 18

Si tratta di un diritto diverso e più esteso dal “blocco” del trattamento di cui all’articolo 7, comma 3, lettera c) del Codice. In particolare è esercitabile non solo in caso di violazione dei presupposti di liceità del trattamento (quale alternativa alla cancellazione degli stessi), bensì anche se l’interessato chieda la rettifica dei dati (in attesa della rettifica da parte del titolare) o si opponga la loro trattamento ai sensi dell’articolo 21 del Regolamento (in attesa di valutazione da parte del titolare). Esclusa la conservazione, ogni altro trattamento di cui si chiede la limitazione è vietato a meno che ricorrano determinate circostanze (consenso dell’interessato, accertamento diritti in sede giudiziaria, tutela diritti di altra fisica o giuridica, interesse pubblico rilevante). Il diritto alla limitazione prevede che il dato personale sia contrassegnato in attesa di determinazioni ulteriori, pertanto è opportuno che i titolari prevedano nei propri sistemi informativi (elettronici o meno) misure idonee a tale scopo.

Diritto alla portabilità dei dati – Articolo 20

Si tratta di uno dei nuovi diritti previsti dal regolamento, anche se non è tutto sconosciuto ai consumatori (si pensi alla portabilità del numero telefonico, per fare un esempio alla portata di tutti).

Non si applica ai trattamenti non automatizzati (quindi non agli archivi o registri cartacei) e sono previste specifiche condizioni per il suo esercizio, in particolare sono portabili solo i dati trattati con il consenso dell'interessato o sulla base di un contratto stipulato con l'interessato (quindi non si applica ai dati il cui trattamento si fonda sull'interesse pubblico o sull'interesse legittimo del titolare per esempio) e solo i dati che siano stati forniti dall'interessato al titolare (si veda considerando 68). Inoltre il titolare deve essere in grado di trasferire direttamente i dati portabili ad un altro titolare indicato dall'interessato, se tecnicamente possibile.

5. ADEMPIMENTI INTERNI

5.1 Il trattamento dei dati

Per comprendere cosa significhi trattamento occorre partire dalla definizione che il GDPR fornisce di dato personale “Qualsiasi informazione riguardante una persona fisica identificata o identificabile (“interessato”); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale”.

Ne discende che per trattamento si intende “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”. E' sufficiente anche una sola delle operazioni elencate per ritenere in corso un trattamento di dati personale.

Il trattamento dei dati deve essere effettuato con modalità atte ad assicurare il rispetto dei diritti e della dignità dell'interessato. Oggetto del trattamento devono essere i soli dati essenziali per svolgere attività istituzionali. I dati personali devono essere trattati in modo lecito raccolti e registrati per scopi determinati, espliciti e legittimi ed utilizzati in operazioni del trattamento in termini non incompatibili con tali scopi.

Il regolamento conferma che ogni trattamento deve trovare fondamento in un'ideale base giuridica.

I fondamenti di liceità del trattamento sono indicati all'articolo 6 del GDPR e coincidono, in linea di massima con quelli che erano previsti dal Codice privacy (consenso, adempimenti contrattuali, interessi vitali della persona interessata o di terzi, obblighi di legge cui è soggetto il titolare, interesse pubblico o esercizio di pubblici poteri, interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati).

Consenso

- per i dati “sensibili” (Articolo 9 del regolamento) il consenso deve essere esplicito, lo stesso dicasi per il consenso a decisioni basate su trattamenti automatizzati (compresa la profilazione - Art. 22);

- non deve essere necessariamente “documentato per iscritto”, né è richiesta la “forma scritta” anche se questa è modalità idonea a configurare l’inequivocabilità del consenso e del suo essere “esplicito” (per i dati sensibili). Inoltre, il titolare (articolo 7.1) deve essere in grado di dimostrare che l’interessato abbia prestato il consenso ad uno specifico trattamento;
- il consenso dei minori è valido a partire dai 16 anni, prima di tale età occorre raccogliere il consenso dei genitori o di chi ne fa le veci;
- deve essere, in tutti i casi, libero, specifico informato e inequivocabile e non è ammesso il consenso tacito o presunto (no a caselle prespuntate su un modulo);
- deve essere manifestato attraverso “dichiarazione o azione positiva inequivocabile” (articoli 39 e 42 del regolamento).

Obblighi legali e conformità legale

La base più severa, precisa, ma anche ottimale per il trattamento dei dati (per quanto riguarda il controllore dei dati) è l’esistenza di almeno una disposizione di legge (considerando 39, 40, 41, articolo 6, paragrafo 1), che richiede (ossia giustifica) la attività di trattamento dei dati. È obbligatorio che i controllori / processori² forniscano prima o al momento della raccolta dei dati le specifiche dell’atto giuridico e il suo estratto numerato

Il considerando 45 e l’articolo 6, paragrafo 1, lettera c), articolo 6, paragrafo 3), estratti del GDPR, consentono il trattamento se è necessario per adempiere a un obbligo legale ai sensi delle leggi dell’UE o di uno Stato membro.

Ci sono molti esempi di queste basi giuridiche: registri di impiego, rapporti sugli incidenti nei registri relativi alla salute e sicurezza, ecc.

Adempimento contrattuale

Il riconoscimento del fondamento stesso delle operazioni commerciali (vale a dire gli obblighi contrattuali) è rappresentato dalla base giuridica (considerando 44, articolo 6, paragrafo 1, lettera b)) che consente il trattamento in due scenari. Innanzitutto, se è necessario per stipulare un nuovo contratto o lavorare in base al contratto esistente con l’interessato, il trattamento dei dati è consentito. Il secondo scenario è quando l’interessato avvia delle attività nei confronti del controllore dei dati, nel qual caso il trattamento è consentito anche prima della stipula del contratto. È il caso dell’esecuzione di misure precontrattuali (preparazione o negoziazione prima di stipulare un contratto), in cui il GDPR sottolinea che l’avvio delle fasi di trattamento dovrebbe essere effettuato su richiesta dell’interessato, anziché essere avviato dal controllore.

Un esempio di questo è il trattamento dei dati della carta di credito per eseguire il pagamento. Nei casi in cui un contratto non è ancora esistente, come quando una persona richiede informazioni a un fornitore di servizi su un particolare servizio via e-mail o social network, il trattamento dei dati personali di quella persona è consentito ai fini della risposta alla richiesta.

Interessi vitali

In situazioni non contemplate dalla legge specifica e in assenza di un contratto, il trattamento è autorizzato se è necessario per la salvaguardia degli interessi vitali dell’interessato (considerando 46, articolo 6, paragrafo 1, lettera d). La condizione può estendersi ad altre persone (ad esempio i figli dell’interessato).

Si consiglia, tuttavia, di fare attenzione all’applicabilità, in quanto gli “interessi vitali” di solito si applicano solo alle situazioni di vita o di morte. Tali situazioni possono includere servizi di emergenza che ricevono un elenco di nomi e età dei residenti al momento di rispondere a una chiamata di emergenza. Questa base giuridica si può invocare solo se nessuna delle altre condizioni di liceità può trovare applicazione (considerando 46).

Compito di interesse pubblico o connesso all'esercizio di pubblici poteri

Quando l'esecuzione di un compito svolto nell'interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare richiede il trattamento di dati personali, è consentito ai sensi del considerando 45; articolo 6, paragrafo 1, lettera e), del GDPR.

Sebbene l'autorizzazione sia concessa di default, il trattamento eseguito su questa base può essere soggetto a obiezione da parte degli interessati. Questa è formalmente riconosciuta, in modo da consentire il riesame delle specifiche della situazione. In sostanza conferisce all'interessato la possibilità di mettere in discussione la definizione di interesse pubblico del titolare. L'obiezione può essere accolta o meno, ma deve essere considerata e deve essere data risposta in modo tempestivo.

Un esempio di questo tipo di trattamento è il caso in cui i partiti politici siano autorizzati a gestire una copia del registro elettorale.

Interessi legittimi

Forse la base giuridica più ambigua per il trattamento è il principio degli "interessi legittimi" (considerando 47, 48, articolo 6, paragrafo 1, lettera f)). In breve, offre la possibilità di sviluppare una giustificazione per il trattamento di dati che non rientrano nei modelli giuridici di cui sopra. Questa giustificazione consentirà il trattamento dei dati evitando la gestione del consenso degli interessati. Può riguardare sia il titolare dei dati sia il terzo a cui i dati verranno comunicati.

Tuttavia, ciò si applica solo in situazioni in cui gli interessi, i diritti o le libertà degli interessati non prevalgono sugli interessi del titolare. Al fine di confrontare questi gruppi di interessi potenzialmente opposti, i titolari devono condurre una cosiddetta "valutazione comparata" (che sarà oggetto di un articolo separato).

Il GDPR fornisce vaghe descrizioni di possibili scenari, che si inseriscono nella base di interessi legittimi. Gli esempi includono: determinati rapporti con i clienti o relativi al servizio tra l'interessato e il titolare (con limitazioni relative ai contratti di lavoro e alle autorità pubbliche). Sono inoltre comprese le procedure per prevenire le frodi, nonché la trasmissione di dati personali all'interno delle imprese dei titolari dei dati o delle istituzioni affiliate a un organismo centrale a fini amministrativi interni. Questo può includere l'elaborazione dei dati personali dei clienti o dei dipendenti.

Il bilanciamento fra legittimo interesse del titolare o di terzi e diritto e libertà dell'interessato non spetta all'Autorità, a è compito dello stesso titolare. Si tratta di una delle principali espressioni del principio di responsabilizzazione del titolare introdotto dal GDPR. Il Regolamento offre alcuni criteri per il bilanciamento in questione (considerando 47).

5.2 Presupposti giuridici per ARS per trattamento dati.

Preliminarmente occorre verificare l'esistenza di legge e regolamento.

Il riferimento per ARS è la legge 24 febbraio 2005, n. 40 e ss.mm. che all'art. 82 *novies decies* prevede che ARS possa accedere a tutti i flussi di dati a carattere regionale attinenti alla salute e al benessere sociale ovunque collocati.

La Regione Toscana, su parere del Garante, ha ritenuto troppo debole e generica questa disposizione e non sufficiente a garantire la legittimità di tutti i trattamenti dell'Agenzia. In primo luogo perché il rinvio che il codice privacy fa alla legge non è a legge regionale (come nel caso della l.r. n. 40/2005), ma a legge nazionale, poi perché il dettato presenta un carattere troppo generico per circoscrivere la legittimità dei trattamenti, che invece devono essere chiari, non generici ed individuati con precisione.

Pertanto per compensare l'insufficienza della legge la RT ha dedicato all'interno del regolamento generale privacy una scheda contenuta nell'allegato A) n. 12 intitolata "Attività di programmazione, gestione, controllo e valutazione dell'assistenza sanitaria" e interamente dedicata ad ARS (allegato A)) scheda n. 12).

All'interno di suddetta sono elencate le operazioni eseguibili nonché la tipologia dei dati che ARS può trattare.

Se il trattamento da effettuare riguarda uno dei dati che sono elencati nel regolamento direttamente o desumibile attraverso la connessione di più flussi, allora è possibile procedere alle operazioni di trattamento dei dati.

Laddove la legge regionale n. 40/2005 unitamente al regolamento forniscano la copertura legittimante suddetto trattamento **ARS è legittimata a trattare il dato.**

A seguito del nuovo regolamento privacy della regione Toscana ARS è titolare dei flussi al pari di quest'ultima ed è stata inserita come legittimo destinatario di tutti i dati che provengono anche alla Regione Toscana.

Per agevolare gli operatori nelle operazioni di trattamento dei dati, con il presente protocollo sono tipizzate quattro fattispecie ricorrenti nell'attività dell'agenzia. Di tutte viene fornito l'inquadramento giuridico che legittima i trattamenti e le indicazioni tecniche. Per la trasmissione delle richieste scritte si allegano anche formulari.

5.3 Fattispecie tipiche.

Per agevolare gli operatori nelle operazioni di trattamento dei dati, con il presente protocollo sono tipizzate le fattispecie più frequentemente ricorrenti nell'attività dell'agenzia. Di tutte viene fornito l'inquadramento giuridico che legittima i trattamenti e le indicazioni tecniche. Laddove si debba ricorrere a richieste scritte si allegato anche formulari.

- 1. Dati aggregati**
- 2. Dati individuali anonimi senza elementi di identificazione diretta (vedi IDUNI)**
- 3. Dati individuali anonimi con elementi di identificazione diretta:**
 - 3 a) quando è sufficiente l'IDUNI**
 - 3 b) quando è necessario il CF**

5.3.1 Fattispecie n. 1

Dati aggregati (massima libertà)

I dati "aggregati non personali" sono le informazioni variamente raccolte e riunite in gruppi di modo che non sia più possibile identificare i singoli utenti. Tali informazioni non consentono di individuare i dati personali dell'interessato.

In questo caso il trattamento non è sottoposto a vincoli né a limitazioni.

5.3.2 Fattispecie n. 2

Dati individuali anonimi senza elementi di identificazione diretta (vedi IDUNI)

La fattispecie. ricorre quando sia necessario acquisire dalle aziende sanitarie alcuni dati che siano stati contrassegnati dall'IDUNI (identificativo universale) o altro codice che rende anonimizzati i dati.

Le aziende sanitarie sono un ente pubblico. Il trasferimento dei dati da ente pubblico ad altro ente pubblico **è consentita se lo prevedono leggi o regolamenti, o risultino comunque necessarie per lo svolgimento di funzioni istituzionali:**

Occorre pertanto verificare se nella scheda n. 12 del regolamento privacy della Regione Toscana siano censiti i dati oggetto del trattamento.

5.3.3 Fattispecie n. 3

Dati individuali anonimi con elementi di identificazione diretta

La fattispecie ricorre quando si devono trattare dati contrassegnati da CF e che rendono quindi conoscibili gli interessati.

Tenuto conto che il CF consente l'individuazione diretta degli interessati e dato che ARS tratta dei dati che afferiscono alla sfera sensibilissima degli individui, occorre fare alcune puntualizzazioni.

Il Codice prevede che i dati relativi allo stato di salute siano anonimi.

Preliminarmente si dovrebbe verificare che gli interessati (che sono coloro cui i dati appartengono es. pazienti delle aa.ss.ll.) abbiano rilasciato il consenso informato. ARS non è tenuta a rilasciare il consenso informato ma solo l'informativa. Il consenso informato è adempimento obbligatorio per gli esercenti le professioni sanitarie e gli organismi sanitari pubblici.

Nel caso in esame, trattandosi di dati provenienti dalle aziende sanitarie, occorre parlare di consenso informato.

Nel consenso informato deve essere inserita l'informativa ove sia precisato tra le altre indicazioni che il dato è raccolto anche ai fini di studio e ricerca scientifica e/o epidemiologica.

Per rappresentare con precisione i contenuti essenziali del consenso informato si allega sub lett. B) il modello che ARS ha predisposto in occasione di progetto.

*Il consenso informato assume un ruolo fondamentale negli **studi prospettici** dato che se non si è provveduto al momento della raccolta del dato a far sottoscrivere il consenso informato, i dati non possono essere trattati.*

A questo punto occorre distinguere due diversi casi a seconda che il dato del CF sia necessario o non necessario per la finalità dell'attività per quale si deve trattare il dato.

a) quando è sufficiente l'IDUNI

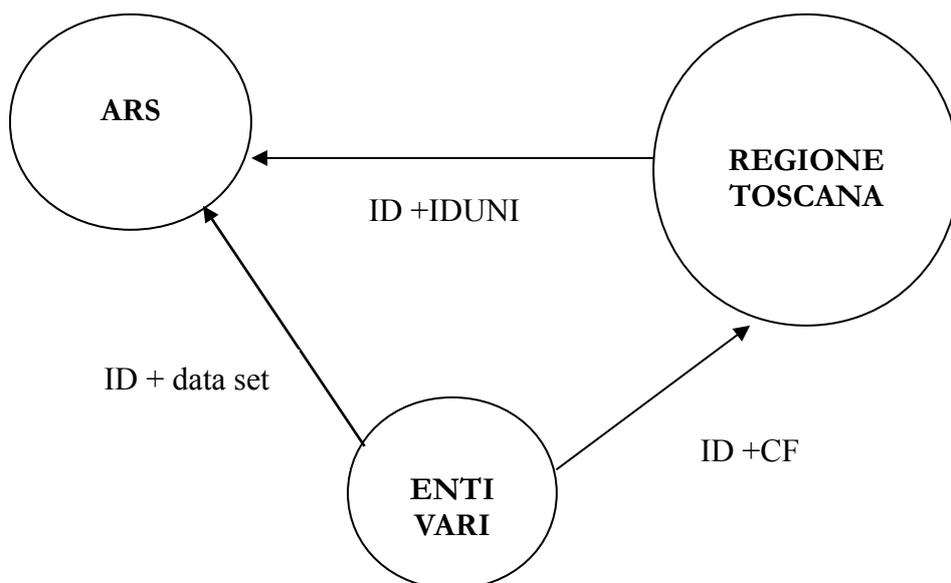
b) quando è necessario il CF

a) quando è sufficiente l'IDUNI

Nel caso in cui dati richiesti alle aziende contrassegnati da CF siano utilmente utilizzabili con IDUNI le possibilità di richiesta sono due.

1. Se la richiesta è fatta alle ASL, le stesse dovrebbero essere autonome nel trasformare l'IDUNI in CF attraverso le proprie strutture competenti.
2. se la richiesta è fatta ad altri enti o le aziende non sono in grado di provvedere alla trasformazione CF-IDUNI, occorre chiedere ai suddetti enti di trasmettere i dati con CF alla Regione Toscana (Responsabile settore sistemi informativi e servizi. Ufficio regionale di statistica Via di Novoli, n. 26 50127 Firenze) affinché provveda alla trasformazione e inoltri ad ARS i dati con IDUNI (si veda modello allegato sub lettera C).

Una volta ottenuto il nulla osta da parte dell'ufficio privacy regionale, ARS, attraverso la PO Statistica e ingegnerizzazione dati sanitari, prenderà contatto con gli uffici regionali tecnici per concordare l'invio dei dati criptati.



b) quando è necessario il CF

Se il dato deve essere utilmente trattato solo con il codice fiscale in chiaro perché altrimenti verrebbe frustrata la finalità dello studio, si procede come di seguito è descritto.

Occorre che il trattamento sia previsto da norma di legge o regolamento; occorre anche sia ottenuto il consenso in cui sia specificato che il dato è raccolto anche fini di studio e ricerca; se non è stato fatto firmare il consenso informato e non è possibile farlo successivamente perché gli interessati sono una collettività indeterminata o non rintracciabili, **ARS non può trattare il dato**. Possono trattarlo solo gli esercenti professioni sanitarie e gli organismi sanitari pubblici purché richiedano una specifica autorizzazione del Garante o il trattamento afferisca all'ambito di applicazione delle autorizzazioni generali del Garante.

A tal proposito, ogni anno il Garante emette delle autorizzazioni di carattere generale.

L'autorizzazione, che riguarda gli esercenti professioni sanitarie e organismi sanitari pubblici, è la n. 2/2014 - Autorizzazione al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale ed è efficace dal 1° gennaio 2015 fino al 31 dicembre 2016 (Gazzetta Ufficiale n. 301 del 30 dicembre 2014).

Il codice privacy previgente, prevedeva l'istituto delle autorizzazioni generali del Garante, per determinate categorie di titolari di trattamento, pubblicate in Gazzetta ufficiale (articolo 40). Al riguardo il decreto opera una precisa distinzione:

- quelle su materie delegate dal Gdpr agli Stati membri – articoli 6 (1), (c) ed (e), 9 (2), (b) e (4), nonché capo IX del Gdpr - sono assoggettate ad una speciale procedura di verifica che può durare circa sette mesi (art. 21 del decreto);
- le altre cessano di avere efficacia dal 19 settembre 2018.

Con Provvedimento n. 497 del 13 dicembre 2018, il Garante per la protezione dei dati personali, in forza dell'art. 21 del d.lgs. 101/2018, ha individuato le disposizioni ancora valide delle Autorizzazioni Generali al trattamento dei dati personali emanate nel 2016, successivamente prorogate (con Provvedimento n. 424 del 19 luglio 2018) nell'attesa che venissero definite le norme di coordinamento con la disciplina europea (GDPR).

Per mezzo delle autorizzazioni generali il Garante permette il trattamento di dati sensibili o giudiziari a determinate condizioni, per determinati fini, e per certe categorie di titolari.

Si può pertanto affermare che l'autorizzazione, in senso generico, costituisce una condizione di liceità del trattamento. È un provvedimento del Garante, il quale, dopo aver valutato la non pericolosità del trattamento, acconsente ad esso.

ARS non è coperta dall'autorizzazione generale del 2016, quindi è necessario procedere alla richiesta di autorizzazione specifica la Garante.

Tenuto conto dei tempi di attesa per il rilascio della stessa è necessario che la richiesta di autorizzazione sia inviata al Garante molto tempo prima dell'inizio del trattamento. Questo rende difficilmente praticabile tale ipotesi.

Una volta ottenuta l'autorizzazione è possibile trattare i dati.

Anche in presenza di consenso informato è obbligatorio chiedere il parere al comitato etico.

Il ruolo dei Comitati etici locali è cruciale per valutare: la qualità e l'opportunità dello studio, l'indipendenza dello studio, i vantaggi che possono derivarne per la popolazione; la qualità della comunicazione al paziente, la comprensione dell'informazione da parte del paziente, la sua libertà e capacità decisionale.

Il compito generale è quello di favorire la presa di coscienza e la messa in pratica dei principi etici da parte della ricerca.

Da un lato, i Comitato etici si occupano di esaminare ed approvare dal punto di vista etico i progetti di ricerca e le pubblicazioni scientifiche, secondo i requisiti invalsi a livello nazionale e internazionale nell'ambito della ricerca scientifica.

D'altro lato, i Comitati etici costituiscono l'organismo preposto a ricevere le segnalazioni di presunti casi di plagio o altro comportamento scientifico scorretto da parte dei ricercatori/sperimentatori.

I Comitati sono chiamati ad intervenire in caso di Sperimentazione Clinica e Sperimentazione Clinica Multicentrica.

Per Sperimentazione Clinica si intende ogni sperimentazione su soggetti umani finalizzata ad identificare o verificare gli effetti clinici, di uno o più medicinali o di procedure terapeutiche non farmacologiche (ad esempio intervento chirurgico, protocollo di radioterapia, dispositivi medici, etc.) in sperimentazione e/o ad identificarne ogni reazione avversa. Nel caso di medicinali sperimentali, la sperimentazione può essere intesa a studiarne gli effetti farmacodinamici, il meccanismo di azione, l'assorbimento, la distribuzione, il metabolismo e l'eliminazione, con l'obiettivo di valutarne la sicurezza e/o l'efficacia. Le sperimentazioni cliniche possono essere "profit" o "no-profit". I termini "sperimentazione clinica" e "studio clinico" sono sinonimi.

La Sperimentazione Clinica Multicentrica è uno studio clinico effettuato seguendo un unico Protocollo in più Centri e per questa ragione condotto da più sperimentatori.

I Comitati Etici hanno anche il compito di:

- monitorare l'andamento degli studi
- promuovere l'informazione e la formazione per medici e pazienti
- fornire pareri e orientamenti nel caso di eventuali richieste specifiche, sia a livello individuale (per esempio cosa conviene fare in casi particolari dove non vi è certezza su quale sia il miglior trattamento da applicare), sia a livello di politiche e pratiche generali (per esempio nel caso in cui si debbano prendere decisioni per gruppi di pazienti).

In Toscana

Il comitato etico regionale per la sperimentazione clinica è un organismo indipendente volto a garantire la tutela dei diritti, della sicurezza e del benessere delle persone inserite nei programmi di sperimentazione svolti nelle strutture del sistema sanitario regionale e a fornire pubblica garanzia di

tale tutela (Delibera Giunta regionale n.418/2013 in attuazione del Decreto Legge n.158/2012 convertito con modificazioni dalla Legge 8 novembre n.189/2012).

5.4 I registri delle attività di trattamento

Il registro delle attività di trattamento è un adempimento che il GDPR pone in capo ai titolari e responsabili del trattamento e che consente di avere una chiara panoramica dei trattamenti di dati personali che vengono effettuati all'interno dell'organizzazione che fa per l'appunto capo al titolare o al responsabile.

L'onere della tenuta del Registro è a carico del titolare o suo delegato e, se nominato, del responsabile del trattamento. La tenuta del registro è utile per una completa ricognizione e valutazione dei trattamenti svolti e quindi finalizzata anche all'analisi del rischio di tali trattamenti e a una corretta pianificazione degli stessi. Il registro deve essere tenuto in forma scritta, anche in formato elettronico, e va esibito all'autorità di controllo in caso di verifiche.

Ai sensi dell'art 30 del GDPR "Registro delle attività di trattamento":

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.

Ad ulteriore precisazione della norma si riporta il considerando 82 del Regolamento.

“Per dimostrare che si conforma al presente regolamento, il titolare del trattamento o il responsabile del trattamento dovrebbe tenere un registro delle attività di trattamento effettuate sotto la sua responsabilità. Sarebbe necessario obbligare tutti i titolari del trattamento e i responsabili del trattamento a cooperare con l'autorità di controllo e a mettere, su richiesta, detti registri a sua disposizione affinché possano servire per monitorare detti trattamenti”.

Come si evince dalle premesse normative, la tenuta dei registri di trattamento si configura come base necessaria al fine di dimostrare la conformità dei trattamenti ai principi enucleati dal GDPR. Preme sottolineare come oltre al titolare la norma richiede che anche il responsabile del trattamento sia tenuto alla redazione di un registro dei trattamenti. Per come si va quindi a configurare, tale strumento di lavoro potrà essere visto sotto un duplice punto di vista: sia come strumento operativo di mappatura dei trattamenti effettuati sia come strumento probatorio che dimostra il pieno adempimento alla normativa.

La norma prevede tuttavia deroghe alla tenuta della documentazione in esame; nel caso in cui l'organizzazione del titolare o del responsabile si sostanzino in realtà con meno di 250 dipendenti non sarà necessaria l'adozione del registro, tuttavia nel caso in cui l'organizzazione al di sotto di tale soglia dimensionale effettui trattamenti che presentino un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale oppure includa il trattamento di dati sensibili o giudiziari, in tal caso è obbligatoria la tenuta dei registri di trattamenti.

La norma indica altresì le informazioni che dovranno confluire nel registro delle attività di trattamento: oltre ai dati di contatto contenuti nella lett. a) art. 30 (titolare, contitolare, rappresentante del titolare e DPO) i dati relativi alle finalità del trattamento, alla descrizione delle categorie di interessati, di dati personali, di destinatari cui i dati saranno comunicati, tra cui rientrano quelli di paesi terzi od organizzazioni internazionali. Nonostante i punti b), c) e d) non siano richiamati con riferimento alle indicazioni contenutistiche cui il responsabile è tenuto, è ragionevole pensare che tali informazioni rientrino nelle “categorie dei trattamenti effettuati per conto del titolare del trattamento”. Non può infatti la definizione di trattamento ignorare l'esatto inquadramento delle finalità del trattamento, categorie di interessati, di dati personali e di destinatari cui i dati saranno comunicati. In ogni caso al responsabile del trattamento non sarà difficile reperire le informazioni di cui alle citate lettere b), c) e d) che saranno invece individuate nell'atto di nomina a responsabile per l'appunto. Una riflessione analoga si può proporre con riguardo alla lett. f) art. 30 in riferimento ai termini previsti per la cancellazione dei dati, essendo anche questa previsione contenuta nell'atto di nomina a responsabile. Di medesimo contenuto invece la previsione dell'individuazione dei soggetti di cui alle lettere a), così come di cui all'art. 30 par. 1 lett. e) e paragrafo 2 lett. c). In entrambe le descrizioni dei registri emerge la presenza della “descrizione generale delle misure di sicurezza tecniche ed organizzative di cui all'art. 32 paragrafo 1”; se da un lato all'atto di designazione di responsabile è obbligatorio indicare che il responsabile “adotti tutte le misure richieste ai sensi dell'art. 32” è altrettanto vero notare come queste non vengano puntualmente definite nella nomina, con la conseguenza di un margine di operatività in capo al responsabile del trattamento dei dati personali in ordine alle misure da adottare; va da sé in altri termini che essendo in potenza difformi tali misure di sicurezza dovranno necessariamente essere presenti nel registro sia del titolare che del responsabile. Sulla scorta di quanto affermato in apertura di commento alla norma secondo cui il registro trattamenti, in un'ottica di accountability, attesta l'adempimento alla normativa va da sé che la possibilità da parte dell'autorità garante di controllo di richiedere che il registro le venga messo a disposizione conferma quanto appena ribadito; su tale direttrice si muove altresì la tenuta in forma scritta dei registri dei trattamenti, ancora una volta infatti la forma scritta consente di adempiere all'onere della prova nel caso in cui si debba eventualmente accertare una forma qualsiasi di responsabilità in capo a titolare oppure al responsabile. La seguente sezione intende fornire una guida per definire le voci presenti nel registro trattamenti che sarà adottato da ARS.

INFORMAZIONI GENERALI

Dati generali del trattamento: insieme di informazioni che identificano il trattamento (codice, denominazione, stato, descrizione)

Soggetti: persone fisiche o giuridiche idonee ad individuare i soggetti attivi del trattamento ed i loro dati di riferimento/identificativi (Titolare o suo delegato/riferimento titolare, contitolare/riferimento contitolare)

Struttura del dirigente titolare del trattamento: dati identificativi (nome proponente) della struttura dirigenziale quale punto di riferimento delegato dal titolare (ufficio/settore cui afferisce, direzione generale, direttore generale, numero decreto nomina, data decreto nomina)

Responsabile esterno del trattamento: dati identificativi del soggetto nominato responsabile esterno ex art. 28 GDPR.

DETTAGLIO TRATTAMENTO

Date significative: individuazione delle date rilevanti ai fini della gestione del trattamento (data compilazione, data validazione, data di inizio validità, data di fine validità)

Fonti normative: indicazione delle fonti normative che individuano/supportano il trattamento

Finalità: individuazione delle finalità di rilevante interesse pubblico perseguite relativamente all'attività istituzionale a cui è collegato il trattamento

Categoria di soggetti associabili: macro categoria di soggetti interessati i cui dati rientrano in un'attività di trattamento del soggetto titolare/responsabile

Modalità di trattamento: indicazione dell'ambito nel quale il trattamento viene posto in essere nonché indicazione del carattere automatizzato o meno del trattamento.

Altre informazioni: informazioni aggiuntive volte in particolare a rivelare se il trattamento può essere definito su "larga scala" o meno.

Operazioni sui dati di cui si compone il trattamento: indicazione delle operazioni svolte sui dati; le operazioni possono essere di carattere standard oppure particolari

Regolamento dei dati sensibili e giudiziari: annotare e citare eventuali codici di condotta o codici deontologici

Consenso e trattamento di dati: indicazioni relative al consenso prestato al trattamento dei dati, all'informativa, al trasferimento ed all'eventuale comunicazione a terzi

ASSET

Strumenti utilizzati: banche dati, tecnologie cloud, strumenti IoT, ecc.

RISCHIO

Dati relativi al rischio: indicazioni volte a quantificare il rischio (sotto un profilo di probabilità di verifica ed impatto) a seguito di trattamento per i diritti e le libertà per l'interessato; successivamente a tale valutazione si decide se procedere a DPIA.

Un'importante funzione di controllo in ordine alla regolare tenuta nonché aggiornamento del registro delle attività di trattamenti è demandata alla figura del DPO.

Ai sensi dell'art. 39 che disciplina infatti le prerogative del soggetto de quo si evince che tra le altre è tenuto a *“sorvegliare l'osservanza del presente 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, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo”*.

All'attribuzione di controllo che gli viene assegnato direttamente dalla legge si aggiunga il già più volte richiamato, nel corso del presente documento, principio di accountability che impone in tal caso al DPO di verificare che l'organizzazione per la quale compie attività di verifica sia conforme

alla disciplina del Regolamento non solo in termini di adempimento, ma anche di capacità di dimostrazione della compliance normative.

Da ultimo si osservi la possibilità di intervento in ordine al controllo sul registro dei trattamenti, potendo intervenire mediante una pluralità di azioni.

Come visto in precedenza per la figura del DPO, sono previsti compiti di sorveglianza per la corretta applicazione del GDPR, anche in capo ai soggetti autorizzati ex art. 29 del GDPR. Soggetti che, per la loro normale attività di trattamento dei dati giornaliera, sono tenuti ad operare una verifica puntuale circa la presenza delle condizioni di liceità del trattamento ex art. 6. nonché del pieno rispetto dei principi applicabili al trattamento di dati ex art. 5 del GDPR durante tutte le fasi che portano all'iscrizione del trattamento sull'apposito registro (censimento, identificazione, verifica di conformità, ecc.).

5.5 La valutazione di impatto privacy

Cos'è la Valutazione di impatto

La DPIA deve avere ad oggetto i rischi rivenienti dalle attività di trattamento dei dati personali che possono causare impatti negativi sui diritti e le libertà delle persone fisiche. A titolo esemplificativo, una errata impostazione del trasferimento telematico dei dati personali della clientela da un titolare ad un altro può comportare la diffusione non autorizzata dei dati stessi.

Nel condurre la valutazione di impatto occorre tuttavia considerare anche la presenza di specifiche condizioni suscettibili di incrementare il rischio del trattamento. L'impiego di tecnologie innovative quali il cloud computing, ad esempio, non è un evento di rischio in sé, ma può incrementare le probabilità di un tale evento, come la diffusione dei dati.

Le indicazioni del Garante privacy

Secondo quanto previsto dal GDPR, il Garante per la privacy ha predisposto un elenco delle tipologie di trattamento – in corso di pubblicazione nella Gazzetta ufficiale – che dovranno essere sottoposte a valutazione di impatto.

Tali tipologie di trattamento – riportate qui in forma sintetica – sono le seguenti:

- a) valutazione o profilazione degli interessati riguardante specifici aspetti, tra i quali: rendimento professionale, situazione economica, stato di salute;
- b) decisioni automatizzate che incidono in misura significativa sull'interessato impedendo di esercitare un diritto o di avvalersi di un servizio (es. verifiche automatizzate per la concessione di un finanziamento);
- c) monitoraggio sistematico degli interessati tramite raccolta di dati relativi alla fruizione di servizi basati su rete telematica (es. monitoraggio della fruizione dei servizi di una piattaforma TV interattiva a fini commerciali o anti-frode);
- d) trattamenti su larga scala di dati aventi carattere estremamente personale (es. corrispondenza e-mail, ubicazione e spostamenti, dati finanziari), nonché scambio di dati personali tra diversi titolari effettuato su larga scala e con modalità telematiche;
- e) attività di monitoraggio tramite sistemi tecnologici dalla quale derivi la possibilità di effettuare un controllo dell'attività dei dipendenti (es. utilizzo di sistemi di videosorveglianza, geolocalizzazione di dotazioni aziendali);
- f) trattamenti non occasionali di dati relativi a soggetti vulnerabili (es. minori, anziani, pazienti);
- g) raffronto di dati personali raccolti per finalità diverse (es. raffronto dei dati di fruizione di servizi digitali con i dati relativi al pagamento);

- h) trattamenti di categorie particolari di dati (es. appartenenza sindacale, stato di salute) oppure di dati relativi a condanne penali e a reati, nonché trattamenti sistematici di dati biometrici o genetici (es. sistemi di accesso con impronta digitale);
- i) utilizzo di tecnologie innovative per il trattamento di dati personali (es. assistenti vocali, smartwatch), in particolare al ricorrere di tipologie di trattamento che possono comportare impatti negativi sui diritti e le libertà delle persone fisiche.

L'elenco completo delle tipologie di trattamento da sottoporre a DPIA è contenuto nel provvedimento del Garante per la privacy all'indirizzo <https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9058979>

Adozione delle indicazioni del Garante privacy

L'elenco di tipologie di trattamento predisposto dal Garante per la privacy non è da considerarsi esaustivo e potrà essere oggetto di integrazione in futuro.

E' possibile dunque che vi siano ulteriori trattamenti per i quali sia richiesta la conduzione di una valutazione di impatto, pur non rientrando questi nelle tipologie anzidette.

Al fine di identificare tali trattamenti, lo stesso provvedimento del Garante richiama due principali riferimenti:

- le Linee guida in materia di valutazione d'impatto sulla protezione dei dati emanate dal Gruppo di Lavoro Articolo 29, nell'ambito delle quali sono definiti una serie di criteri per l'individuazione dei trattamenti da sottoporre a DPIA (il documento è disponibile all'indirizzo http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236);
- le più generali previsioni del GDPR – di cui all'art. 35 comma 1 – che stabilisce l'obbligo di effettuare, prima dell'inizio del trattamento, una valutazione dell'impatto laddove quest'ultimo possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, "allorché preveda in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità [...]".

Come provvedere alla DPIA

L'obbligo di condurre la valutazione di impatto decorre dal 25 maggio 2018. La DPIA deve essere svolta sia per i nuovi trattamenti, sia per quelli che possono presentare un rischio elevato a seguito di variazioni intervenute nelle caratteristiche e modalità.

La normativa fornisce alcune indicazioni di carattere generale in merito ai criteri e alle metodologie da impiegare per la valutazione dei rischi e delle relative misure da implementare, tra le quali quelle citate in precedenza.

5.6 Il registro delle violazioni di dati personali (processo di Data Breach)

A partire dal 25 maggio 2018, tutti i Titolari del trattamento – pubblici e privati – devono notificare all'autorità di controllo ("Garante") le violazioni di dati personali di cui vengano a conoscenza, entro 72 ore e comunque "senza ingiustificato ritardo", ma soltanto se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati (si veda considerando 85). 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 o suo delegato. Se la probabilità di tale rischio è elevata, si dovrà informare delle violazioni anche gli interessati, sempre "senza ingiustificato ritardo"; fanno eccezione le circostanze indicate al paragrafo 3 dell'art. 34. I contenuti della notifica all'autorità e della comunicazione agli interessati sono indicati, in via non esclusiva, agli artt. 33 e 34 del regolamento. Tutti i titolari di trattamento dovranno in ogni caso documentare le violazioni di dati personali subite, anche se non notificate all'autorità di controllo e non comunicate agli interessati, nonché le relative circostanze e conseguenze e i provvedimenti adottati (si veda art. 33, paragrafo 5); tale obbligo non è diverso,

nella sostanza, da quello attualmente previsto dall'art. 32-bis, comma 7, del Codice per gli operatori di comunicazioni elettroniche. I titolari di trattamento devono pertanto adottare le misure necessarie a documentare eventuali violazioni, essendo peraltro tenuti a fornire tale documentazione, su richiesta, al Garante in caso di accertamenti.

Ai sensi dell'art. 4 par. 12 «violazione dei dati personali» ovvero per Data Breach si definisce: “*la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati*”.

La gestione degli incidenti è in carico al Security Manager che:

- a) registra l'incidente
- b) avvisa il titolare dei trattamenti coinvolti
- c) provvede ad una valutazione dell'incidente in termini di gravità con la collaborazione del dirigente/i coinvolto/i nel trattamento/i
- d) Provvede a relazionare al DPO per la decisione relativa alla segnalazione al garante, alla segnalazione agli interessati, alla segnalazione all'autorità giudiziaria se trattasi di atto potenzialmente doloso.

I dirigenti responsabili per ambiti di competenza alla sicurezza IT o titolari di contratti in essere per la fornitura di servizi IT debbono assicurare:

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

Si rinvia al documento sul processo Data Breach.

6. ALTRI ADEMPIMENTI

6.1. IL trasferimento di dati all'estero

In primo luogo con il nuovo Regolamento è venuto meno il requisito dell'autorizzazione nazionale (si vedano articoli 45, paragrafo 1 e 46 paragrafo 2). Ciò significa che il trasferimento verso un Paese terzo adeguato ai sensi della decisione assunta in futuro alla Commissione ovvero sulla base di clausole contrattuali modello, debitamente adottate, o di norme vincolanti l'impresa approvate attraverso la specifica procedura prevista dall'articolo 47 del GDPR, potrà avere inizio senza attendere l'autorizzazione del Garante – a differenza di quanto previsto dall'articolo 44 del Codice. Tuttavia l'autorizzazione del Garante sarà ancora necessaria se il titolare utilizza clausole contrattuali ad hoc (cioè non riconosciute come adeguate tramite decisione della commissione europea) oppure accordi amministrativi stipulati da autorità pubbliche – una delle novità introdotte da Regolamento.

Il GDPR consente di ricorrere anche ai codici di condotta ovvero a schemi di certificazione per dimostrare le “garanzie adeguate” previste dall'articolo 46. Ciò significa che i titolari o i

responsabili del trattamento stabiliti in un Paese terzo potranno far valere gli impegni sottoscritti attraverso l'adesione al codice di condotta o allo schema di certificazione, ove questi disciplinino anche o esclusivamente i trasferimenti di dati verso Paesi terzi, al fine di legittimare tali trattamenti. Tuttavia (si vedano articoli 40, paragrafo 3 e articolo 42, paragrafo 2), tali titolari dovranno assumere, inoltre, un impegno vincolante mediante uno specifico strumento contrattuale o altro strumento che sia giuridicamente vincolante o azionabile dagli interessati.

Il GDPR vieta trasferimenti di dati verso titolari o responsabili in un Paese terzo sulla base di decisioni giudiziarie o ordinanze amministrative emesse da autorità di tale Paese terzo, a meno dell'esistenza di accordi internazionali in particolare di mutua assistenza giudiziaria o analoghi accordi fra Stati (articolo 48). Si potranno utilizzare, tuttavia, gli altri presupposti ed in particolare le deroghe previste per situazioni specifiche di cui all'articolo 49. A tale riguardo, si deve ricordare che il Regolamento chiarisce come sia lecito trasferire i dati personali verso un Paese terzo non adeguato "per importanti motivi di interesse pubblico", in deroga la divieto generale, ma deve trattarsi di un interesse pubblico riconosciuto dal diritto dello Stato membro del titolare o dal diritto UE (articolo 49, paragrafo 4) – e dunque non può essere fatto valere l'interesse pubblico dello Stato terzo ricevente.

Il GDPR fissa i requisiti per l'approvazione delle norme vincolanti d'impresa e i contenuti obbligatori di tali norme. L'elenco indicato al riguardo nel paragrafo 2 dell'articolo 47 non è esaustivo e, pertanto, potranno essere previsti dalle autorità competenti, a seconda dei casi, requisiti ulteriori. Ad ogni modo, l'approvazione delle norme vincolanti d'impresa dovrà avvenire esclusivamente attraverso il meccanismo di coerenza, di cui agli articoli 63 – 65 del GDPR – ossia, è previsto in ogni caso l'intervento del Comitato europeo per la protezione dei dati (si veda articolo 65, paragrafo 1, lettera d)).

Il Capo V del GDPR ha confermato l'approccio che vigeva nella direttiva 95/46 e al Codice privacy per quanto riguarda i flussi di dati al di fuori dell'Unione europea e dello spazio economico europeo, prevedendo che tali flussi sono vietati, in linea di principio, a meno che intervengano specifiche garanzie che il Regolamento elenca in modo gerarchico:

- i) adeguatezza del Paese terzo riconosciuta tramite decisione della Commissione europea;
- ii) in assenza di decisioni di adeguatezza della Commissione, garanzie adeguate di natura contrattuale o pattizia che devono essere fornite dai titolari coinvolti (fra cui le norme vincolanti d'impresa – BCR e clausole contrattuali modello);
- iii) in assenza di ogni altro presupposto, utilizzo di deroghe al divieto di trasferimento applicabili in specifiche situazioni.

Le decisioni di adeguatezza sinora adottate dalla Commissione (livello di protezione dati in Paesi terzi, partire dal Privacy Shield e clausole contrattuali tipo per titolari e responsabili) e gli accordi internazionali in materia di trasferimento dei dati stipulati prima del 24/05/2016 dagli Stati membri rimangono in vigore fino alla loro eventuale revisione o modifica (articoli 45, paragrafo 9 e 96). Restano valide, conseguentemente le autorizzazioni nazionali sinora emesse dal Garante successivamente a tali decisioni di adeguatezza della Commissione (<http://garanteprivacy.it/home/provvedimenti-normativa/normativa/normativa-comunitaria-e-internazionale/trasferimento-dei-dati-verso-paesi-terzi#1>)

Restano valide, inoltre, le autorizzazioni nazionali che il Garante ha rilasciato in questi anni per specifici casi (articolo 46, paragrafo 5, sino a loro eventuale modifica).

6.2. Clausole contrattuali del titolare

Nell'ambito dell'attività contrattuale dell'Agenzia, al fine dell'individuazione delle diverse categorie di rapporti che il contratto o convenzione viene ad instaurare si seguono i seguenti passi fin dalla predisposizione del bando se necessario:

- a) Descrizione del servizio richiesto
- b) Identificazione dei diversi servizi oggetto dell'appalto,
- c) Valutare se e quali servizi comportano l'applicazione del GDPR rilevando se vengono trattati dati personali,
- d) analisi dei servizi e riconducibilità ad una categoria come da tabella precedente. È possibile che un contratto/convenzione riguardi più servizi e che questi si riferiscano a categorie diverse. pertanto potranno anche esserci più DPA per un contratto/convenzione.

Qualora al bando preveda la sottoscrizione di contratto o convenzione, sarà in questi che saranno inserite gli articoli che regoleranno i rispettivi ruoli e responsabilità in termini di data protection, nel caso che il bando non preveda la stipula di un atto susseguente (vedi ad esempio Finanziamenti su progetti) la DPA relativa dovrà essere presente nel bando e ne dovrà essere richiesta la compilazione e la firma da parte del contraente e l'invio congiuntamente all'offerta di servizi/progetto pena la non sua valutazione.

Vale la pena ricordare che il GDPR richiede obbligatoriamente la redazione e sottoscrizione di un accordo fra le parti nel caso di un rapporto che preveda lo scambio di dati personali e più in generale il loro trattamento.

A supporto della classificazione nella corrispondente categoria, si fa riferimento ai contenuti della tabella sopracitata. In particolare, gli elementi distintivi riportati per ogni categoria hanno l'obiettivo di:

- a) guidare l'autore del documento nel definire le ipotesi in cui un servizio può essere collocato in più categorie;
- b) favorire l'esplicitazione delle misure specifiche che dovranno necessariamente essere riportate nel documento finale.

Gli esempi riportati sono solo esemplificativi, durante l'applicazione del GDPR si provvederà a fornire altri esempi inserendo i nuovi contratti e relativi DPA.

In caso non fosse possibile ricondurlo ad alcuna delle categorie predeterminate o in ipotesi in cui il Dirigente abbia difficoltà nell'effettuare tale attività, è tenuto a rivolgersi immediatamente all'Ufficio del DPO presso ARS.

Contenuti da esplicitare nel bando, nel contratto o nella convenzione

In caso si accerti che il servizio comporti attività rilevanti ai sensi di quanto disposto dal GDPR dovranno essere inseriti nel disciplinare di gara, contratto, convenzione, contenuti conformi alle prescrizioni del GDPR”, “Prescrizioni comportamentali per le risorse umane coinvolte”, “Prescrizioni Data Protection per risorse organizzative”, “Prescrizioni per le risorse tecnologiche – misure di sicurezza”).

Tali regolazioni fanno parte dei contenuti dei diversi Data Protection Agreement di cui

- 1) DPA Titolare Responsabile-(sub responsabile) ALLEGATO 15
- 2) DPA Fra titolari autonomi, ALLEGATO 16
- 3) DPA di Contitolarità, ALLEGATO 17

Nel caso dell'appalto di servizi, convenzioni o protocolli di intesa, nei quali non siano previsti trattamenti di dati personali, ma per i quali esiste un rischio di interferenza con trattamenti del Titolare o del Responsabile, il DPA deve prevedere prescrizioni e clausole che riducano il rischio di interferenza, e qualora si concretizzi lo sanzionino.

Per rischio di interferenza si intende l'occasionale accesso a dati personali da parte di persone non coinvolte nel relativo trattamento. Queste sono persone che devono essere istruite affinché pur potendolo fare, non mettano in atto comportamenti che possano produrre Data Breach o incidenti di sicurezza.

7. LE SANZIONI

Con l'entrata in vigore del **GDPR**, il **quadro sanzionatorio privacy** è ben più severo, non soltanto per ciò che riguarda l'entità degli importi, ma anche per quanto concerne le ipotesi per cui possono essere comminate le sanzioni. Prima di esaminare più in dettaglio il funzionamento del mutato quadro regolatorio, va messa in evidenza la scelta del legislatore europeo di uniformare la tipologia e l'entità delle sanzioni, a differenza di quanto accadeva in precedenza, fornendo ex ante alcuni criteri per la ponderazione delle sanzioni amministrative pecuniarie.

Il **Working Party Articolo 29** ha così ritenuto necessario emanare delle linee guida, affinché venisse garantita, da un lato, l'applicazione coerente delle norme sulla protezione dei dati personali, dall'altro, un regime di protezione dei dati armonizzato per tutti i cittadini europei.

Sulla base dell'articolo 82 del GPRD resta fatta salva la possibilità per l'interessato, che subisca un danno materiale o immateriale, di ottenere il risarcimento del danno, a seconda che la violazione sia stata commessa dal Titolare o dal Responsabile.

7.1 **GDPR: le sanzioni amministrative pecuniarie e/o penali**

Il GDPR, agli articoli successivi, invece, disciplina le ipotesi per cui è prevista l'applicazione di sanzioni amministrative pecuniarie e/o penali. Per quanto riguarda le prime esse possono raggiungere i 10 milioni di euro o, se superiore, il 2% del fatturato mondiale nei casi di, a titolo esemplificativo:

- | |
|---------------------------------------------------------------------------------------------------------------------------|
| - violazione delle condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione; |
| - trattamento illecito di dati personali che non richiede l'identificazione dell'interessato; |
| - mancata o errata notificazione e/o comunicazione di un data breach all'Autorità nazionale competente; |
| - violazione dell'obbligo di nomina del DPO; |
| - mancata applicazione di misure di sicurezza. |

L'importo delle **sanzioni amministrative pecuniarie** può salire fino a 20 milioni di euro, o alternativamente, sino al 4% del fatturato mondiale dell'impresa nei casi di, a titolo esemplificativo:

- | |
|---------------------------------------------------------------------------------------------------------------------------------------------------|
| - inosservanza di un ordine, di una limitazione provvisoria o definitiva concernente un trattamento, imposti da un'Autorità nazionale competente; |
| - trasferimento illecito cross-border di dati personali ad un destinatario in un Paese terzo. |

Nonostante il GDPR focalizzi la propria attenzione, prevalentemente, sulle violazioni di tipo amministrativo, all'interno del Considerando 149 è stabilito che gli Stati Membri "dovrebbero poter stabilire disposizioni relative a sanzioni penali" come strumento di attuazione e tutela della nuova disciplina, pur sempre in ossequio al principio del *ne bis in idem*.

All'interno del GDPR è presente anche un margine di discrezionalità circa la possibilità di infliggere una sanzione e la determinazione dell'importo della stessa. Ciò non implica un'autonomia gestionale delle sanzioni in capo alle Autorità nazionali competenti, ma fornisce, a queste ultime, alcuni criteri su come interpretare le singole circostanze del caso. Nello specifico, verranno esaminati di seguito alcuni criteri per la determinazione delle sanzioni amministrative pecuniarie, di cui all'articolo 83 paragrafo 2

- | |
|--------------------------------------------------------------------------------------------------------------------------------------------|
| - "la natura, gravità e durata della violazione"; |
| - "il carattere doloso o colposo della violazione"; |
| - "il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attuarne i possibili effetti negativi". |

Con riferimento al primo criterio, lo stesso regolamento riconosce l'esistenza di diversi massimali per le sanzioni amministrative pecuniarie, i.e. 10 o 20 milioni di euro. Sarà, perciò, compito dell'Autorità nazionale competente valutare le circostanze di specie, alla luce di tali criteri generali, e poi decidere se procedere con una misura correttiva, più o meno severa, sotto forma di sanzione pecuniaria. All'interno del Considerando 148 è offerta all'Autorità nazionale l'opportunità di sostituire la sanzione pecuniaria con un ammonimento, "in caso di violazione minore o se la sanzione pecuniaria che dovrebbe essere imposta costituisca un onere sproporzionato per una persona fisica". Anche tale inciso dimostra la tendenza del legislatore europeo di incoraggiare l'utilizzo delle sanzioni pecuniarie con un approccio "ponderato" ed "equilibrato". L'obiettivo ultimo rimane, infatti, quello di incentivare le società al rispetto della **privacy by design** e **privacy by default**, affidando lo strumento dell'applicazione di sanzioni pecuniarie così elevate, esclusivamente, al fine di reagire in maniera dissuasiva e proporzionata ad eventuali violazioni.

Con riferimento al secondo criterio, le valutazioni, circa l'esistenza di dolo o di colpa nella condotta, verranno effettuate sulla base di elementi oggettivi e sarà compito della giurisprudenza emergente definire ex ante "linee di demarcazione più chiare per valutare il carattere doloso di una violazione". Il Working Party ha, tuttavia, già provveduto ad esemplificare alcune condotte che potranno integrare il suddetto **carattere doloso**. Queste sono riconducibili alle ipotesi di:

- trattamenti illeciti autorizzati esplicitamente dal senior management, ovvero ignorando i pareri formulati dal DPO;
- modifica di dati personali, avente la finalità di fornire un'impressione "fuorviante" circa il conseguimento degli obiettivi individuati;
- vendita di dati, in mancanza di verifica e/o ignorando la scelta liberamente esercitata dagli interessati.

Nello specifico, le sanzioni previste dal Regolamento Privacy Europeo (UE/2016/679) di seguito sono riportate tutte le sanzioni (c.d. multe) previste dal Regolamento Europeo che, ai sensi dell'art. 83 del Reg. UE/2016/679 devono avere carattere di effettività, proporzionalità e dissuasività.

Le sanzioni amministrative pecuniarie riportate nell'elenco che segue, possono essere integrative, oppure completamente sostitutive delle sanzioni correttive indicate nell'elenco successivo e si distinguono in sanzioni di carattere economico e sanzioni correttive.

La decisione sull'applicazione delle sanzioni spetta all'autorità di controllo (in Italia: l'Autorità Garante per la Protezione dei Dati Personali), che, nella valutazione, tiene conto delle circostanze del singolo caso, ossia:

- della natura, gravità e durata della violazione
- del carattere doloso o colposo della violazione
- delle misure adottate per attenuare il danno subito dagli interessati
- delle eventuali precedenti violazioni commesse dal titolare del trattamento
- del grado di cooperazione con l'autorità di controllo
- degli eventuali altri fattori aggravanti

SANZIONI DI CARATTERE ECONOMICO

Inosservanza degli obblighi del titolare e del responsabile del trattamento; inosservanza degli obblighi dell'organismo di certificazione; inosservanza degli obblighi dell'organismo di controllo:

fino a 10 milioni di Euro, o per le imprese, fino al 2% del fatturato annuo mondiale dell'esercizio precedente.

Inosservanza dei principi base del trattamento; inosservanza dei diritti degli interessati; inosservanza delle disposizioni sul trasferimento dei dati personali in paesi terzi o verso organizzazioni internazionali; inosservanza di un ordine, limitazione provvisoria o definitiva o di un ordine di sospensione dei flussi da parte dell'autorità di controllo:

fino a 20 milioni di Euro, o per le imprese, fino al 4% del fatturato annuo mondiale dell'esercizio precedente.

Inosservanza di un ordine correttivo dell'autorità di controllo:

fino a 20 milioni di Euro, o per le imprese, fino al 4% del fatturato annuo mondiale dell'esercizio precedente.

SANZIONI CORRETTIVE:

Le sanzioni correttive sono connesse ai poteri dell’Autorità di controllo. Essi consistono nel:

Rivolgere avvertimenti al titolare del trattamento o al responsabile del trattamento sul fatto che i trattamenti previsti possono violare il GDPR

Rivolgere ammonimenti al titolare e del trattamento o al responsabile del trattamento ove i trattamenti abbiano violato le disposizioni del GDPR

Ingiungere al titolare del trattamento o al responsabile del trattamento di soddisfare le richieste dell’interessato di esercitare i relativi diritti

Ingiungere al titolare o al responsabile del trattamento di conformare i trattamenti alle disposizioni del GDPR, anche specificando in che modo ed entro quale termine

Ingiungere al titolare del trattamento di comunicare all’interessato una violazione dei dati personali

Imporre una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento

Ordinare la rettifica, la cancellazione di dati personali o la limitazione del trattamento e la notificazione di tali misure ai destinatari cui sono stati comunicati i dati personali

Revocare la certificazione o ingiungere all’organismo di certificazione di ritirare la certificazione rilasciata a norma degli articoli 42 e 43, oppure ingiungere all’organismo di certificazione di non rilasciare la certificazione se i requisiti per la certificazione non sono o non sono più soddisfatti

Infliggere una sanzione amministrativa pecuniaria in aggiunta alle presenti misure (v. sopra)

Ordinare la sospensione dei flussi di dati verso un destinatario in un paese terzo o un’organizzazione internazionale.

8. PROTEZIONE DEI DATI E RICERCA IN AMBITO SANITARIO

Prima di tutto è necessario sottolineare che questo è un quadro molto complesso e composito, che vede uno scenario normativo «magmatico» ed in costante evoluzione. Spesso inoltre mancano delle risposte sempre affidanti. Diventa quindi necessario esaminare caso per caso. Il GDPR prevede un regime che affianca garanzie a deroghe nell’ambito della ricerca sanitaria: secondo l’art. 1, par. 1, lett. b: «i dati 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»).

La base legittima del trattamento si ritrova nei seguenti articoli:

art. 6, par. 1, lett. e GDPR (vedi anche Cons. 156-157): *“il trattamento è 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”*;

art. 9 – par. 2, lett. J *“il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell’articolo 89, paragrafo 1, sulla base del diritto dell’Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l’essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell’interessato”* – par. 4 *“Gli Stati membri possono mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute.”*

Come scenario normativo di riferimento, di seguito vengono elencati le diverse norme:

art. 89 GDPR, Titolo V «Trattamenti a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici», artt. 97 – 110bis Codice Privacy – Capo III - Trattamento a fini statistici o di ricerca scientifica, Allegato 1 *“Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica”* 19 dicembre 2018, Prescrizioni relative al trattamento dei dati genetici (aut. gen. n. 8/2016), Prescrizioni relative al trattamento dei dati personali effettuato per scopi di ricerca scientifica (aut. gen. n. 9./2016), Regolamento UE 536/2014 sulla sperimentazione clinica di medicinali per uso umano, Linee guida per i trattamenti di dati personali nell’ambito delle sperimentazioni cliniche di medicinali - 24 luglio 2008, Regolamenti dei Comitati etici, Codici deontologici europei (a livello europeo ci sono dei tavoli di lavoro che stanno lavorando su questo), ecc.

In particolare, si cita l’art. **89 del Regolamento** «Garanzie e deroghe relative al trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici» che prevede

l'assunzione di misure tecniche e organizzative. Guardando poi il nostro Codice Privacy, di seguito, tra gli altri gli articoli che interessano la materia della ricerca in ambito sanitario:

- **art. 106** «Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica», con il quale il Garante promuove regole deontologiche per i soggetti pubblici e privati volte a individuare garanzie adeguate per i diritti e le libertà dell'interessato in conformità all'articolo 89 del Regolamento

- **art. 107** «Trattamento di particolari categorie di dati» che sancisce che il consenso dell'interessato al trattamento di dati di cui all'articolo 9 del Regolamento, quando è richiesto, può essere prestato con modalità semplificate, individuate dalle regole deontologiche di cui all'articolo 106.

- **art. 110** «Ricerca medica, biomedica ed epidemiologica» secondo cui il consenso dell'interessato per il trattamento dei dati relativi alla salute, a fini di ricerca scientifica in campo medico, biomedico o epidemiologico, non è necessario quando la ricerca è effettuata in base a disposizioni di legge o regolamento o al diritto dell'Unione europea in conformità all'articolo 9, paragrafo 2, lettera j), del Regolamento, ivi incluso il caso in cui la ricerca rientri in un programma di ricerca biomedica o sanitaria.

Il consenso non è inoltre necessario quando, a causa di particolari ragioni, informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità di ricerca (ad esempio alle indagini dei big data analitici per cui è molto difficile effettuare la ricerca).

In tali casi, il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, il programma di ricerca è oggetto di motivato parere favorevole del competente comitato etico a livello territoriale e deve essere sottoposto a preventiva consultazione del Garante ai sensi dell'articolo 36 del Regolamento. In caso di esercizio dei diritti dell'interessato ai sensi dell'articolo 16 del Regolamento nei riguardi dei trattamenti di cui al comma 1, la rettificazione e l'integrazione dei dati sono annotati senza modificare questi ultimi, quando il risultato di tali operazioni non produce effetti significativi sul risultato della ricerca.

- **art. 110-bis:** articolo molto discusso, contestabile perché incontra delle difficoltà sistematiche. Sancisce il trattamento ulteriore da parte di terzi dei dati personali a fini di ricerca scientifica o a fini statistici. Introduce quindi l'obbligo di richiesta al Garante per l'autorizzazione: “Il Garante può autorizzare il trattamento ulteriore di dati personali, compresi quelli dei trattamenti speciali di cui all'articolo 9 del Regolamento, a fini di ricerca scientifica o a fini statistici da parte di soggetti terzi che svolgano principalmente tali attività quando, a causa di particolari ragioni, informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca, a condizione che siano adottate misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, in conformità all'articolo 89 del Regolamento, comprese forme preventive di minimizzazione e di anonimizzazione dei dati. Il Garante comunica la decisione adottata sulla richiesta di autorizzazione entro quarantacinque giorni, decorsi i quali la mancata pronuncia equivale a rigetto. on il provvedimento di autorizzazione o anche successivamente, sulla base di eventuali verifiche, il Garante stabilisce condizioni e le misure necessarie ad assicurare adeguate garanzie a tutela degli interessati nell'ambito del trattamento ulteriore dei dati personali da parte di terzi, anche sotto il profilo della loro sicurezza. Il Garante può anche autorizzare mediante provvedimenti generali.

Per quanto riguarda le regole deontologiche, ai sensi dell'Art. 20, comma 4, del d.lgs. 10 agosto 2018, n. 101 -19 dicembre 2018 (ex Allegato 4), non si applicano ai trattamenti per scopi statistici e scientifici connessi con attività di tutela della salute svolte da esercenti professioni sanitarie od organismi sanitari, ovvero con attività comparabili in termini di significativa ricaduta personalizzata sull'interessato, che restano regolati dalle pertinenti disposizioni. Vengono infine affrontati alcuni aspetti che meritano attenzione in relazione alle criticità che possono emergere durante la gestione di un progetto di ricerca.

Necessario determinare misure organizzative atte a gestire le varie fasi di sviluppo dell'attività di progetto, individuare quindi il ruolo delle divisioni e dei comitati coinvolti (Comitato etico e/o Comitato ricerca), stabilire un corretto workflow interno, dare enfasi su accountability (tramite soluzioni anche di carattere documentale). Necessario è anche attenzionare la gestione dei ruoli privacy

nel progetto di ricerca: definire quindi una corretta mappatura dei flussi di dati, stabilire la titolarità ed eventuale contitolarità, nomina di responsabili.

9 DIPOSIZIONI FINALI

Le presenti prescrizioni sono aggiornate a seguito dell'evoluzione del quadro normativo di riferimento, nonché a seguito dell'emanazione da parte del Garante di ulteriori disposizioni in materia.

Il titolare, con il supporto dell'Ufficio DPO presso ARS, è tenuto a adeguare le prescrizioni da impartire agli incaricati sulla base dell'aggiornamento del presente documento.