



CONSIGLIO REGIONALE DELLA PUGLIA

Deliberazione dell'Ufficio di Presidenza del Consiglio

N. 200 del registro delle deliberazioni

OGGETTO: Regolamento (UE) 2016/679 - Protezione dei dati personali di Titolarità del Consiglio regionale. Attribuzione di funzioni e compiti ai Designati al trattamento e istruzioni alle persone autorizzate, ai sensi dell'art. 2-quaterdecies del D.Lgs. 196/2003.

L'anno 2018, addì 11 del mese di Dicembre, in Bari, nella residenza del Consiglio, previo regolare invito, si è riunito l'Ufficio di Presidenza nelle persone dei Signori:

		PRES.	ASS.	
Presidente del Consiglio	:	Mario Cosimo LOIZZO	SI	
Vice Presidente del Consiglio	:	Giuseppe LONGO	SI	
“ “ “	:	Giacomo Diego GATTA	SI	
Consigliere Segretario	:	Giuseppe TURCO	SI	
“ “ “	:	Luigi MORGANTE	SI	

Constatata la presenza del numero legale per la validità della seduta, il Presidente Mario Cosimo Loizzo assume la presidenza e dichiara aperta la stessa.

Assiste il Segretario generale del Consiglio, avv. Domenica Gattulli.

Il Presidente del Consiglio Regionale, Mario Cosimo Loizzo, sulla base dell'istruttoria espletata dalla Dirigente del Servizio Affari Generali e confermata dal Segretario Generale del C.R., riferisce quanto segue.

Il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 "Regolamento Generale sulla Protezione dei dati", noto anche come *General Data Protection Regulation* (GDPR), pubblicato sulla GUCE del 4 maggio 2016 ed in vigore dal 25 maggio 2018, con l'abrogazione della direttiva 1995/46/CE, costituisce il nuovo asse portante del quadro normativo eurounitario.

Sul punto si ricorda che il Legislatore nazionale con legge n. 163/2017 ("Legge di delegazione europea 2016-2017") ha delegato il Governo ad adottare uno o più provvedimenti per adeguare il D.Lgs. 196/2003 "Codice in materia di protezione dei dati personali", alle norme del citato Regolamento.

La legge delega è stata attuata con D.Lgs. 101/2018 recante "*Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)*", che ha allineato la normativa italiana al quadro comunitario, apportando modifiche, abrogazioni e disposizioni di dettaglio al D.Lgs.196/2003.

Tra le novità introdotte da Regolamento, si richiama la previsione del principio di "*accountability*" ossia di "responsabilizzazione", che impone al Titolare di dimostrare di aver adempiuto agli obblighi a tutela della protezione dei dati personali che discendono dal regolamento e dalla disciplina nazionale.

Il Titolare è definito all'art. 4 del Regolamento (UE) 2016/679 come "*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*".

Per i trattamenti facenti capo al Consiglio regionale, lo stesso riveste, per definizione di legge, il ruolo di Titolare del trattamento, non mutando in sostanza il ruolo di vertice nell'assetto organizzativo privacy dallo stesso ricoperto, nella vigenza del precedente quadro normativo.

Il Consiglio regionale in qualità di Titolare è responsabile del rispetto del Regolamento n. 679/16 all'interno del proprio ente e deve mettere in atto tutte le misure tecniche ed organizzative idonee a garantire la protezione dei dati personali trattati, dimostrandone l'adozione.

Rispetto alle nuove misure di tipo organizzativo poste in essere a seguito dell'entrata in vigore del Regolamento (UE) 2016/679, si ricorda la deliberazione dell'Ufficio di Presidenza n. 162 del 24 maggio 2018 con cui è stato istituito il registro delle attività di trattamento, previsto dall'art. 30 del Regolamento, e la nomina del Responsabile della protezione dei dati personali (RPD), prevista dall'art. 37 dello stesso Regolamento, di cui alla deliberazione dell'Ufficio di Presidenza n. 159 del 21 giugno 2018 nonché la partecipazione del Consiglio regionale al gruppo di lavoro regionale per la protezione dei dati personali, costituito a supporto del RPD, con Deliberazione della Giunta n. 794/2018.

E' opportuno altresì, dopo la prima fase di applicazione del Regolamento ed in vista dell'imminente trasferimento della sede del Consiglio regionale della Puglia, che si proceda a cura della struttura ICT ad una revisione delle policy in tema di sicurezza ai sensi dell'art. 32 del Regolamento (UE) 2016/679, che tenga conto anche delle nuove componenti dell'infrastruttura tecnologica che sarà impiegata per il trattamento dei dati personali, e ad una verifica dell'adeguatezza delle misure di sicurezza in essere, con eventuale adeguamento delle stesse.

Sotto un profilo strettamente organizzativo, afferente ai ruoli che intervengono nel trattamento, si evidenzia che il Regolamento (UE) 2016/679, all'art. 4, introduce la figura delle "persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare", prevedendo al successivo art. 29 che esse siano istruite prima di poter trattare dati personali.

Con il regolamento, viene meno la figura del "Responsabile interno" e degli "Incaricati" al trattamento. Tuttavia l'art. 2-quaterdecies del D.Lgs. 196/03, come novellato dal D.lgs. 101/18, espressamente prevede che il Titolare sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, possa attribuire a persone fisiche, espressamente designate, che operano sotto la sua autorità, specifici compiti e funzioni connessi al trattamento, individuando le modalità più opportune per l'autorizzazione al trattamento di dati personali.

Il Consiglio regionale opera attraverso le figure amministrative di vertice, legate da un rapporto di interorganicità con l'ente, che attuano il programma politico con atti di gestione amministrativa e finanziaria, a seconda delle specifiche competenze attribuite alle strutture medesime e dell'incarico conferito ai Dirigenti responsabili delle stesse.

Si ritiene pertanto conforme a quanto disposto dal Regolamento e dal novellato Codice Privacy, nonché coerente con un modello di articolazione di responsabilità su delega, su cui si fonda l'organizzazione degli enti complessi, e nello specifico, l'organizzazione dello stesso Consiglio regionale, delegare i Dirigenti o i soggetti ad essi equiparati, legati da un rapporto di interorganicità con l'ente, al trattamento di dati personali conseguenti all'esercizio dell'incarico ricevuto, qualificandoli quali "Designati" al trattamento.

I Dirigenti per essere autorizzati al trattamento dei dati personali nell'ambito delle funzioni istituzionali svolte e prima di avviare un trattamento di dati personali, devono ricevere dal Titolare, secondo quanto previsto dal richiamato art. 29 del Regolamento, le istruzioni necessarie a garanzia della correttezza delle operazioni di trattamento.

Con il presente provvedimento si intende pertanto: aggiornare l'assetto organizzativo privacy del Consiglio regionale e nello specifico autorizzare i Dirigenti del Consiglio a trattare, per conto del Titolare, i dati personali nell'ambito delle funzioni istituzionali svolte e dell'incarico affidato e attribuire ad essi i compiti specifici declinati nel documento "Compiti e istruzioni per il designato al trattamento dei dati personali ai sensi dell'art. 2-quaterdecies del D.Lgs. 196/03" allegato sub A del presente provvedimento e facente parte integrante dello stesso.

Tanto premesso, Il Presidente invita, quindi, l'Ufficio di Presidenza a deliberare al riguardo.

ADEMPIMENTI CONTABILI DI CUI ALLA L.R. N. 28/2001 E AL REGOLAMENTO DI
AMMINISTRAZIONE E CONTABILITA' DEL CONSIGLIO REGIONALE
LA PRESENTE DELIBERAZIONE NON COMPORTA IMPLICAZIONI DI NATURA
FINANZIARIA

L'UFFICIO DI PRESIDENZA

Udita e fatta propria la relazione del Presidente Mario Cosimo Loizzo;
VISTO il Reg. (UE) 2016/679
VISTO IL D.Lgs. 196/13
VISTO lo Statuto Regionale;
VISTO l'art. 59 della L.R. n. 1 del 7/02/2004;
VISTA La L.R. n. 7 del 12/05/2004;
VISTA la LR. n. 6 del 21/03/2007, recante norme sull'autonomia del Consiglio regionale;
VISTI gli artt. 25 e 26 del Regolamento di Organizzazione del Consiglio regionale adottato con deliberazione dell'Ufficio di Presidenza n. 39 del 20.4.2016;
VISTA la sottoscrizione posta in calce alla presente deliberazione;

All'unanimità dei voti espressi nei modi di legge;

DELIBERA

Per le motivazioni riportate in narrativa che qui si intendono integralmente riportate:

- di delegare, per le ragioni indicate in premessa, i Dirigenti del Consiglio regionale della Puglia e i soggetti ad essi equiparati, ciascuno per quanto di propria competenza, a trattare i dati personali nello svolgimento dell'incarico ricevuto e pertanto di individuarli quali "Designati" al trattamento;
- di approvare il documento "*Compiti e istruzioni per il designato al trattamento dei dati personali ai sensi dell'art. 2-quaterdecies del D.Lgs. 196/03*" di cui all'**allegato A** del presente provvedimento, che costituisce parte integrante e sostanziale del presente provvedimento;
- di demandare a ciascun "Designato" al trattamento l'applicazione di quanto contenuto nel documento sub A e specificatamente l'autorizzazione al trattamento del personale assegnato e del personale che con lo stesso collabora, che tratti dati personali, utilizzando il modello di autorizzazione unito all. A;
- di delegare il Dirigente della struttura ICT, Responsabile della sicurezza, alla revisione delle policy in tema di sicurezza ai sensi dell'art. 32 del Regolamento (UE) 2016/679, che tenga conto anche delle nuove componenti dell'infrastruttura tecnologica che sarà impiegata presso la futura sede del Consiglio regionale, e ad una verifica dell'adeguatezza delle misure di sicurezza in essere, con eventuale implementazione delle misure ulteriori che si ritenessero necessarie;
- di trasmettere il presente provvedimento ai Dirigenti del Consiglio regionale e al Responsabile per la protezione dei dati personali;
- di pubblicare il presente provvedimento sul sito web del Consiglio regionale e sulla bacheca elettronica del Consiglio regionale.

Il Segretario generale del Consiglio
Avv. Domenica Gattulli



Il Presidente
Cosimo Mario Loizzo



Le sottoscritte attestano che il procedimento istruttorio affidato loro è stato espletato nel rispetto della vigente normativa regionale, statale e comunitaria e secondo le direttive dell'Ufficio di Presidenza e che il presente provvedimento, dalla stessa predisposto, è conforme alle risultanze istruttorie.

Il Dirigente del Servizio Affari Generali

Avv. Maria Conte



Il funzionario istruttore

dott.ssa Marialucia Beneveni



ALLEGATO A

Compiti e Istruzioni
per il Designato al trattamento
dei dati personali

ai sensi dell'art. 2-quaterdecies del D.Lgs. 196/03

Consiglio Regionale della Puglia
Titolare del trattamento

SOMMARIO

Premessa.....	3
Quadro normativo generale	3
Finalità.....	3
PARTE PRIMA	4
Disposizioni generali	4
1. Vocabolario necessario.....	4
2. Condizioni di liceità del trattamento (art.6 del Regolamento europeo).....	6
3. La comunicazione e la diffusione di dati personali	7
4. Il trattamento di categorie particolari di dati personali e dei dati relativi alle condanne penali e ai reati (art. 9 e 10 del Regolamento europeo).....	8
5. Principi applicabili al trattamento dei dati (art. 5, 24 e 25 del Regolamento europeo)	9
6. Il ventaglio di diritti degli interessati (art. 12-23 del Regolamento Europeo)	10
7. L'Informativa (artt. 13 e 14 del Regolamento europeo)	12
8. Il Responsabile della protezione dei dati (art. 37 del Regolamento europeo)	13
9. Il registro delle attività di trattamento (artt. 30 del Regolamento europeo)	14
10. La sicurezza dei dati – Indicazioni generali (art. 32 del Regolamento Europeo).....	15
11. L'analisi dei rischi (art. 32, par. 2, del Regolamento Europeo)	15
12. La valutazione d'impatto (art. 35 del Regolamento europeo).....	17
13. Databreach e registro dei databreach (art. 33 e 34 del Regolamento Europeo).....	17
PARTE SECONDA	19
14. L'assetto organizzativo privacy del Consiglio regionale.....	19
15. I compiti del Designato al trattamento.....	21
Appendice	24
Elenco Trattamenti dati personali del Consiglio Regionale della Puglia - Registro ex art. 30 Reg.679/16 (D.U.P. 162/2018)	25
Allegato A.1.....	28
Allegato A.2.....	31

PREMESSA

QUADRO NORMATIVO GENERALE

Il 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", pubblicato nella Gazzetta Ufficiale dell'Unione Europea, serie L 119 del 04.05.2016, noto come General Data Protection Regulation (GDPR), da ora in poi definito "Regolamento europeo", è direttamente applicabile negli Stati membri dell'Unione Europea a decorrere dal **25 maggio 2018**.

Il Regolamento europeo, all'art. 94, par. 1, dispone l'abrogazione della Direttiva 95/46/CE. La legge n. 163/2017, all'art. 13, ha attribuito al Governo la delega ad adottare uno o più provvedimenti per adeguare le disposizioni del D. Lgs. n.196/2003, recante *Codice in materia di protezione dei dati personali*, in contrasto o incompatibili con la disciplina delineata dal Regolamento europeo.

In attuazione della predetta delega, con Decreto Legislativo 10 agosto 2018, n. 101, la normativa nazionale è stata adeguata alle disposizioni del Regolamento europeo e numerosi articoli del D. Lgs. n.196/2003, aventi ad oggetto la disciplina di aspetti normati dal Regolamento europeo, sono stati abrogati.

Di seguito riferendo del D. Lgs. n.196/2003, come modificato da ultimo dal D. Lgs. n.101/2018, si utilizzerà l'abbreviazione "Codice".

Ulteriori norme che disciplinano la materia della protezione dei dati personali e che integrano il quadro normativo di riferimento sono contenute nelle linee guida, nei pareri adottati dall'Autorità di controllo nazionale (d'ora in avanti "Garante della privacy"), nonché nelle regole deontologiche di cui all'art. 2-*quater* del Codice, promosse e approvate dallo stesso Garante della privacy.

Si rammenta che alcuni di questi provvedimenti sono stati adottati in epoca antecedente all'entrata in vigore del Regolamento europeo e pertanto, pur esplicitando ancora la loro efficacia, essi andranno reinterpretati e attuati alla luce della nuova disciplina.

Si segnalano alcune importanti novità introdotte dal Regolamento Europeo: l'istituzione del registro delle attività di trattamento (art. 30); la tenuta del registro degli incidenti o registro databreach (art. 33), la designazione di un Responsabile della protezione dei dati (art. 37), la valutazione di impatto (art. 35).

FINALITÀ

Con il presente documento, il Consiglio regionale della Puglia, Titolare del trattamento, intende fornire ai Dirigenti del Consiglio regionale ("Designati al trattamento") direttive e istruzioni per i trattamenti di dati personali effettuati, con richiami alle norme applicabili allo specifico ambito di attività agli stessi attribuito, fermo restando che il Regolamento europeo deve essere comunque rispettato in tutte le sue parti, anche se non richiamate in questa sede.

Si precisa che la disciplina rilevante in materia di protezione dei dati personali si compone anche delle indicazioni e delle linee guida fornite dal Garante della privacy.

Sono resi disponibili in allegato al documento: a) il modello di autorizzazione al trattamento di dati personali, per il personale assegnato alla struttura; b) il modello di Informativa ai sensi degli artt. 13 e 14 del Regolamento europeo.

Di questo documento dovrà essere data la più ampia diffusione al personale del Consiglio regionale, ponendolo a corredo dell'autorizzazione al trattamento che i Dirigenti dovranno consegnare al personale operante presso la propria struttura.

PARTE PRIMA

DISPOSIZIONI GENERALI

1. Vocabolario necessario.

Ai fini del Regolamento europeo, a norma dell'art. 4, si intende per:¹

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;
3. "profilazione", qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
4. "pseudonimizzazione", il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

¹ si riportano solo alcune delle definizioni di cui all'art. 4.

5. "archivio", qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
6. "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;
7. "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;
8. "destinatario", la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;
9. "terzo", la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
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. "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;
12. "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;
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;
14. "autorità di controllo", l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51.

Si notino le seguenti novità introdotte dal Regolamento europeo e recepite dal legislatore nazionale con il D. Lgs. n. 101/2018:

- ✓ Il "responsabile del trattamento", di cui all'art. 28 del Regolamento europeo, è figura decisamente differente dal "responsabile", come individuato all'art. 4, comma 1, lett. g, e all'art. 29 del D. Lgs. n. 196/2003 (entrambi gli articoli sono stati oggetto di abrogazione).
- ✓ Il Regolamento europeo non contempla la definizione di "dati sensibili", di "dati giudiziari", di "dati anonimi" e di "incaricati", né il ruolo del "responsabile del trattamento" come definito dal d.lgs. 196/03;

- ✓ Per quanto concerne i “dati sensibili”, il Regolamento europeo, riferendosi ad essi, li qualifica all’art. 9 come "*categorie particolari di dati personali*". Essi sono i dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, nonché i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona. Si può notare tuttavia una sostanziale corrispondenza tra le due qualificazioni: quella di “dati sensibili” e quella di “categorie particolari di dati personali”.
- ✓ Per quanto attiene i “dati giudiziari”, il Regolamento europeo all’art 10, rubricato "*Trattamento dei dati personali relativi a condanne penali e reati*", non fornisce alcuna definizione relativamente a detta tipologia di dati. Parimenti il Codice non fornisce di questa tipologia di dati un’elencazione più dettagliata, a differenza di quanto previsto dall’art. 4, lett. e), del D.Lgs. 196/03, oggi abrogato dal D.lgs. 101/18.
- ✓ Con riferimento ai “dati anonimi”, si segnala quanto disposto dall’art. 11 "*Trattamento che non richiede l’identificazione*", che disciplina la fattispecie di trattamento che non richiede (o non richiede più) l’identificazione dell’interessato.
- ✓ La figura dell’ “incaricato” è sostituita dal soggetto “autorizzato”, che si trova menzionato quasi per inciso all’art. 4, n.10, e a cui si riferisce l’art. 29 "*Trattamento sotto l’autorità del titolare del trattamento o del responsabile del trattamento*". L’autorizzato (al pari del “vecchio” incaricato) è colui che agisce sotto l’autorità del titolare.

2. Condizioni di liceità del trattamento (art.6 del Regolamento europeo)

Prima di attivare un trattamento, è necessario porsi la domanda sull’esistenza di presupposti che rendano lecito il trattamento che si intende effettuare.

L’articolo 6 del Regolamento europeo stabilisce le condizioni di liceità del trattamento, senza distinguere tra la natura privata o pubblica del titolare del trattamento. Sono pertanto ricomprese condizioni applicabili e condizioni non applicabili ad una Pubblica Amministrazione.

All’art. 6, nell’ordine di esposizione delle condizioni di liceità, si annovera quale prima voce il consenso prestato dall’interessato. Tanto farebbe apparire il consenso, quale condizione di liceità di carattere generale, anche per i trattamenti svolti da un soggetto pubblico. E tanto costituirebbe una sostanziale novità rispetto a quanto statuito dal D.Lgs. 196/03 che – si ricorda - all’art. 18 non lo contemplava tra i presupposti di legittimità dei trattamenti in ambito pubblico e che, specificatamente al comma 4 del citato art. 18, fatta eccezione per i soggetti esercenti servizi sanitari, disponeva che "*i soggetti pubblici non devono richiedere il consenso dell’interessato*".

In realtà anche nel nuovo quadro normativo, il consenso non appare una generale condizione di liceità del trattamento svolto da un soggetto pubblico, se si legga il Considerando n. 43 che così recita: <<Per assicurare la libertà di espressione del consenso, è opportuno che **il consenso non costituisca un valido presupposto per il trattamento dei dati personali in un caso specifico, qualora esista un evidente squilibrio tra l’interessato e il titolare del trattamento, specie quando il titolare del trattamento è un’autorità pubblica** e ciò rende pertanto improbabile che il consenso sia stato espresso liberamente in tutte le circostanze di tale situazione specifica. [...]>>.

Possono tuttavia verificarsi situazioni specifiche in cui l'ente pubblico, nel perseguire l'interesse posto alla base della propria azione amministrativa, di fatto agisca *more privatorum* (ad esempio per l'organizzazione di convegni, per pubblicazioni audio-video a fini promozionali o culturali, etc.). In tali fattispecie, spesso caratterizzate dall'assenza di una esplicita base giuridica legittimante il trattamento, in ottemperanza al principio di responsabilizzazione (vd. Paragrafo 5), si suggerisce, in ogni caso, di raccogliere e documentare la volontà dell'interessato rispetto al trattamento svolto.

Premesso quanto sopra, le condizioni di liceità dei trattamenti rilevanti per la Pubblica Amministrazione sono rinvenibili là dove:

1. *"il trattamento è necessario per adempiere un **obbligo legale** al quale è soggetto il titolare del trattamento"* (art. 6, par. 1, lett. c);
2. *"il trattamento è necessario per l'esecuzione di un **compito di interesse pubblico connesso all'esercizio di pubblici poteri** di cui è investito il titolare del trattamento"* (art. 6, par. 1, lett. e);

L'art. 2-ter del Codice rubricato *"Base giuridica per il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri"*, in attuazione di quanto disposto dall'art. 6, par. 3, lett. b), del Regolamento europeo, dispone che la base giuridica su cui si fonda il trattamento è costituita esclusivamente da una norma di legge o, nei casi previsti dalla legge, di regolamento.²

3. La comunicazione e la diffusione di dati personali

Quando il trattamento è costituito dalla comunicazione o dalla diffusione, in considerazione della delicatezza di queste operazioni, il Codice detta una normativa più stringente.

La comunicazione è il dare conoscenza dei dati personali in qualunque forma (mettendoli a disposizione, in consultazione, con interconnessione tra banche dati) a uno o più soggetti determinati (diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione europea, dal responsabile o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate).

La diffusione è il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

L'art. 2-ter del Codice prevede al comma 2 che *"la comunicazione fra titolari che effettuano trattamenti di dati personali, diversi da quelli ricompresi nelle particolari categorie di cui all'articolo 9 del Regolamento e di quelli relativi a condanne penali e reati di cui all'articolo 10 del Regolamento, per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri è ammessa se prevista ai sensi del comma 1."*, ossia in presenza di una norma di legge o, nei casi previsti dalla legge, di regolamento.

"In mancanza di tale norma – continua l'art. 2-ter - la comunicazione è ammessa quando è comunque necessaria per lo svolgimento di compiti di interesse pubblico e lo svolgimento di funzioni istituzionali e può

² Il Regolamento europeo <<non impone che vi sia un atto legislativo specifico per ogni singolo trattamento. Un atto legislativo può essere sufficiente come base per più trattamenti effettuati conformemente a un obbligo legale cui è soggetto il titolare del trattamento o se il trattamento è necessario per l'esecuzione di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri>> (vedi Considerando n. 45).

essere iniziata se è decorso il termine di quarantacinque giorni dalla relativa comunicazione al Garante, senza che lo stesso abbia adottato una diversa determinazione delle misure da adottarsi a garanzia degli interessati”.

Lo stesso art. 2-ter, al comma 3, stabilisce che *“La diffusione e la comunicazione di dati personali, trattati per l’esecuzione di un compito di interesse pubblico o connesso all’esercizio di pubblici poteri, a soggetti che intendono trattarli per altre finalità [es: la comunicazione a soggetti privati] sono ammesse unicamente se previste ai sensi del comma 1”* e quindi solo in presenza di una norma di legge o di regolamento, non trovando applicazione il meccanismo della comunicazione al Garante, di cui al capoverso precedente.

La comunicazione di dati rientranti nella categoria di cui all’art. 9 del Regolamento europeo (già dati sensibili) e all’art. 10 dello stesso (già dati giudiziari) può avvenire solo in presenza di una norma di legge o di regolamento che specifichi i contenuti stabiliti rispettivamente dall’art. 2-sexies e dall’art. 2-octies.

Fermo restando quanto sopra detto, la diffusione dei dati genetici, biometrici e relativi allo stato di salute è espressamente vietata dall’art. 2-septies del Codice.

Si richiamano le *“Linee Guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati”* (adottate dal Garante della privacy con Del. 243/14 e pubblicate in G.U. n. 134 del 12.6.2014) che forniscono indicazioni operative sulla pubblicazione di atti contenenti dati personali.

4. Il trattamento di categorie particolari di dati personali e dei dati relativi alle condanne penali e ai reati (art. 9 e 10 del Regolamento europeo).

Il trattamento di categorie particolari di dati personali (vd. art.9 del regolamento europeo) di per sé è vietato, salvo casi specifici elencati allo stesso art. 9.

Per quanto riguarda il Titolare soggetto pubblico, il trattamento è consentito se *“necessario per motivi di interesse pubblico rilevante³ sulla base del diritto dell’Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l’essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell’interessato”* (art. 9, par. 2, lett. g).

Il Codice, con riferimento ai trattamenti di particolari categorie di dati ex art. 9, ha disposto con l’art. 2-sexies che: *“I trattamenti delle categorie particolari di dati personali di cui all’articolo 9, paragrafo 1, del Regolamento, necessari per motivi di interesse pubblico rilevante ai sensi del paragrafo 2, lettera g), del medesimo articolo, sono ammessi qualora siano previsti dal diritto dell’Unione europea ovvero, nell’ordinamento interno, da disposizioni di legge o, nei casi previsti dalla legge, di regolamento che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell’interessato”.*

³ L’art. 2-sexies, al comma 2, indica alcuni trattamenti qualificati ex lege di rilevante interesse pubblico, svolti da soggetti con compiti di interesse pubblico (es: accesso a documenti amministrativi, tenuta di registri di stato civile e anagrafe della popolazione, concessione e revoca benefici economici etc).

Il successivo art. 2-octies del codice, con riguardo ai trattamenti di dati relativi a condanne penali e reati ex art. 10 del regolamento europeo, che non avvengano sotto il controllo di un'autorità pubblica, prevede la liceità degli stessi se autorizzati da una norma di legge o di regolamento ovvero se individuati con Decreto del Ministero della Giustizia. Tipicamente i trattamenti autorizzati riguardano gli ambiti definiti all'art. 2-octies, c. 3, (es: adempimenti di obblighi ed esercizio diritti in materia di lavoro da parte del titolare; verifica o accertamento requisiti di onorabilità; adempimenti di obblighi in materia di informazione e comunicazione antimafia, etc.). La legge, il regolamento o il Decreto del Ministero di Giustizia, che individuano i trattamenti ammessi, dispongono altresì le misure e le garanzie appropriate per i diritti e le libertà degli interessati.

Ad oggi, l'attività del Consiglio regionale della Puglia è stata svolta sotto l'egida del regolamento regionale n. 5 del 25 maggio 2006, con cui l'amministrazione regionale ha individuato, ai sensi dell'art. 20 e dell'art. 21 del D.Lgs. 196/03 le attività il cui svolgimento comporta il trattamento di dati sensibili e giudiziari, individuando dati e operazioni. Detto regolamento dovrà essere oggetto di prossimo aggiornamento per adeguarlo alla vigente normativa.

5. Principi applicabili al trattamento dei dati (art. 5, 24 e 25 del Regolamento europeo)

Individuata la sussistenza di una delle condizioni di liceità di cui ai precedente paragrafi, ogni trattamento di dati personali deve avvenire nel rispetto primario di alcuni **principi di ordine generale**, indicati dall'art. 5 del Regolamento europeo, ai sensi del quale *"I dati personali sono:*

- 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; [...] («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»).*

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

L'art. 5, par. 2, del "Regolamento europeo" di fatto introduce il concetto di **compliance** (di matrice anglosassone), richiedendosi al Titolare di comprovare la congruenza dei propri trattamenti al Regolamento europeo. Questo concetto è legato al principio di "responsabilizzazione" (**accountability**) che costituisce una delle principali novità rispetto al regime previgente.

Viene affidato ai Titolari il potere di decidere autonomamente le modalità del trattamento dei dati personali, soprattutto sotto il profilo della sicurezza, pur nel rispetto delle disposizioni normative che definiscono inderogabilmente il perimetro di garanzia e i limiti nel trattamento.

Nell'attuale quadro normativo, vengono meno le cd. "misure minime di sicurezza", elencate nell'all. B al D. Lgs 196/03, che, se da un verso guidavano e rassicuravano il Titolare rispetto agli obblighi di sicurezza da rispettare, per altro verso, avrebbero potuto costituire una misura non necessariamente adeguata.

La nuova impostazione presuppone una riconosciuta maturità e competenza del Titolare nel trattare i dati personali. Un complemento importante, che discende dal principio di "responsabilizzazione", è la necessità che il Titolare sia in grado di **documentare ogni adempimento e ogni misura tecnica o organizzativa adottata (compliance)**.

Chi tratta dati personali ha il compito di mettere in atto comportamenti proattivi e tali da dimostrare la concreta adozione di misure, finalizzate ad assicurare l'applicazione del Regolamento europeo (anche ai fini di dover riscontrare richieste informative da parte del Garante della Privacy).

Il "Regolamento Europeo" codifica due nuovi principi che risentono della pervasività del digitale nelle attività di gestione dei processi aziendali. L'art. 25 introduce i principi di **Privacy by design** e di **Privacy by default**. Il primo dei due principi impone (sia al momento di determinare i mezzi di trattamento, sia all'atto del trattamento stesso) di mettere *"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"*⁴.

Il secondo principio impone che *"che siano trattati, per impostazione predefinita ["by default"], 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"*.

6. Il ventaglio di diritti degli interessati (art. 12-23 del Regolamento Europeo)

L'interessato ha diritto di ricevere dal Titolare le informazioni e le comunicazioni relative al trattamento che lo riguardano in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro. Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici (**art. 12, par. 1 del Regolamento europeo**).

⁴ Ai fini dell'applicazione del principio del privacy by design, è rimessa al Titolare una valutazione discrezionale che dovrà tenere conto dello stato dell'arte, dei costi di attuazione, del contesto e delle finalità del trattamento, della probabilità e gravità del rischio per i diritti e le libertà delle persone fisiche.

Il Titolare, a fronte di una richiesta avanzata dall'Interessato ai sensi del Capo III del Regolamento Europeo, deve dare riscontro senza ingiustificato ritardo e, comunque, **al più tardi entro un mese** dal ricevimento della stessa. Tale termine, se necessario, può essere prorogato di due mesi tenuto conto della complessità e del numero delle richieste. L'interessato deve essere informato di tale proroga, e dei motivi del ritardo, entro un mese dal ricevimento della richiesta (art. 12, par. 3).

Nel caso in cui non sia possibile ottemperare alla richiesta dell'Interessato, questi ha diritto di ricevere notizia senza ritardo, e al più tardi entro un mese dal ricevimento della sua richiesta, dei motivi dell'inottemperanza nonché della possibilità di proporre reclamo al Garante della privacy e di proporre ricorso giurisdizionale (art. 12, par.4).

Il Titolare del trattamento deve fornire preventivamente all'interessato le informazioni sul trattamento. Trova applicazione l'art. 13, qualora i dati personali siano raccolti presso l'interessato e l'art. 14 qualora i dati personali non siano ottenuti presso l'interessato. Le informative dovranno essere complete, dotate di un linguaggio chiaro, semplice e adeguato allo scopo cui sono dirette (**Diritto all'informativa, artt. 13 – 14**).

L'interessato ha diritto di ottenere dal Titolare la conferma che sia in corso o meno un trattamento di dati personali che lo riguardano e in tal caso di accedere a questi e alle informazioni che li riguardano (**Diritto di accesso dell'interessato art. 15**). Si noti come le voci oggetto dell'accesso siano sostanzialmente rispondenti alle voci da fornire con l'Informativa. D'altronde si tratta di diritti in posizione complementare. Tanto più complete sono le informative, tanto minore sarà lo spazio informativo da colmare per riscontrare un'istanza di accesso dell'interessato.

L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano, senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa (**art.16 Diritto di rettifica e di integrazione**).

L'interessato ha il diritto di ottenere la **cancellazione** dei dati personali che lo riguardano senza ingiustificato ritardo, se sussiste uno dei motivi indicati **all'art. 17**, comma 1. Il **diritto all'oblio** (che nasce da fonte giurisprudenziale) consiste nel **diritto di un individuo a non essere più ricordato**. Nel caso dei trattamenti effettuati da un soggetto pubblico, deve ricorrere una delle condizioni indicate al citato art. 17, comma 1.⁵

E' altresì riconosciuto all'interessato il diritto di chiedere la limitazione del trattamento quando ricorrano le condizioni descritte all'**art. 18 (Diritto di limitazione del trattamento)**.

Nelle ipotesi di rettifica, cancellazione e limitazione dei dati, l'Interessato ha diritto che il Titolare porti a conoscenza di ciascuno dei destinatari a cui i dati personali sono stati comunicati, le eventuali rettifiche o cancellazioni o limitazioni del trattamento dei dati che lo riguardano, *"salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato"* (**art. 19**).

⁵ "a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati; b) ...c) ...d) i dati personali sono stati trattati illecitamente; e) i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento; f) ...".

L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano effettuato ai sensi dell'articolo 6, par.1, lett. e) ossia quando il trattamento sia reso "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". In tal caso, "il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria" (art. 21, par.1). Su questo punto – ad integrazione di quanto sopra – è opportuno prendere visione anche del Considerando n. 69 che così recita: "Qualora i dati personali possano essere lecitamente trattati, essendo il trattamento necessario per l'esecuzione di **un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri** di cui è investito il titolare del trattamento, ovvero per i legittimi interessi di un titolare del trattamento o di terzi, l'interessato dovrebbe comunque avere il diritto di opporsi al trattamento dei dati personali che riguardano la sua situazione particolare. È opportuno che incomba al titolare del trattamento **dimostrare che i suoi interessi legittimi cogenti prevalgono sugli interessi o sui diritti e sulle libertà fondamentali dell'interessato.**" (art. 21 Diritto di opposizione)

7. L'Informativa (artt. 13 e 14 del Regolamento europeo)

Il diritto all'informativa garantisce alla persona di **conoscere, generalmente prima dell'inizio del trattamento, l'ambito di circolazione dei propri dati, le finalità, il soggetto o i soggetti decidenti e di procedere su tale base a un consapevole esercizio dei poteri di controllo**, come ad esempio, l'espressione o il diniego del consenso o il diritto di opposizione (laddove applicabili).

A tal fine l'informativa va data **prima di effettuare la raccolta dei dati** e in essa devono essere specificate le seguenti informazioni:

- a) titolare del trattamento (Consiglio regionale della Puglia): indirizzo e sede;
- b) designato del trattamento: indirizzo e dati di contatto (pec/e-mail, tel.);
- c) responsabile della protezione dei dati (DPO): indirizzo, mail e tel.;
- d) le finalità del trattamento e la base giuridica del trattamento;
- e) i destinatari dei dati personali o eventuali categorie di destinatari;
- f) eventuale trasferimento dei dati personali in Paesi terzi e, in caso affermativo, attraverso quali strumenti;
- g) periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione;
- h) i diritti dell'interessato (il diritto di accesso, diritto di rettifica, diritto di cancellazione, diritto di limitazione di trattamento, diritto di opposizione, diritto alla portabilità dei dati);
- i) il diritto di proporre reclamo al Garante della privacy;
- j) le possibili conseguenze per il mancato conferimento dei dati;
- k) se il trattamento comporta processi decisionali automatizzati (anche la profilazione), l'informativa deve specificarlo e deve indicare anche la logica di tali processi decisionali e le conseguenze previste per l'interessato.

L'art. 13, par. 3, prescrive che "Qualora il titolare del trattamento intenda **trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti**, prima di tale ulteriore trattamento

fornisce all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente”, (cd. **informativa ulteriore**).

Qualora i **dati non siano stati ottenuti presso l'interessato**, ai sensi dell'art. 14, è obbligatorio integrare l'informativa con l'indicazione (cd. **informativa successiva**):

1. delle categorie di dati in questione (art. 14, par. 1, lett. d);
2. 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, par.2, lett. f).

Il titolare deve fornire l'informativa all'Interessato **non oltre un mese** dall'ottenimento dei dati; nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato, al momento della prima comunicazione; se invece è prevista la comunicazione ad altro destinatario, non oltre la prima comunicazione dei dati personali a questi (art. 14. par. 3).

Sono previste **eccezioni all'obbligo di rendere l'informativa** (art. 13, par. 4 e art. 14, par. 5), “*se e nella misura in cui*”:

a) *l'interessato dispone già delle informazioni;*

b) *comunicare tali informazioni risulta impossibile o implicherebbe uno sforzo sproporzionato; in particolare per il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatte salve le condizioni e le garanzie di cui all'articolo 89, paragrafo 1, o nella misura in cui l'obbligo di cui al paragrafo 1 del presente articolo rischi di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità di tale trattamento. In tali casi, il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, anche rendendo pubbliche le informazioni;*

c) *l'ottenimento o la comunicazione sono espressamente previsti dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento e che prevede misure appropriate per tutelare gli interessi legittimi dell'interessato; oppure*

d) *qualora i dati personali debbano rimanere riservati conformemente a un obbligo di segreto professionale disciplinato dal diritto dell'Unione o degli Stati membri, compreso un obbligo di segretezza previsto per legge.*

In calce all'Informativa può essere richiesta una firma all'interessato esclusivamente “*per presa visione*” e non come autorizzazione/consenso al trattamento⁶.

8. Il Responsabile della protezione dei dati (art. 37 del Regolamento europeo)

Il Responsabile della protezione dei dati, anche noto come “Responsabile della protezione dei dati” (RPD) e “Data Protection Officer” (DPO), è una nuova figura, con compiti di informazione e consulenza per il titolare

⁶ Una parziale deroga alla regola predetta è rinvenibile nel trattamento di immagini e filmati per i quali si preveda la diffusione, in particolare nel caso di dati personali di minori. Il Regolamento europeo all'art. 8 prescrive che, qualora il trattamento si basi sul consenso, “*il trattamento di dati personali del minore è lecito ove il minore abbia almeno 16 anni. Ove il minore abbia un'età inferiore ai 16 anni, tale trattamento è lecito soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare della responsabilità genitoriale*”. Sul punto si richiama quanto precisato in tema di consenso al paragrafo 2.

e di sorveglianza del rispetto del Regolamento europeo. Per svolgere dette funzioni, il RPD deve essere coinvolto in tutte le questioni riguardanti la protezione di dati personali e deve ricevere la più ampia collaborazione da parte del titolare. Svolge le sue funzioni in piena autonomia e risponde esclusivamente al vertice gerarchico del titolare. Rappresenta il punto di contatto sia per il Garante della Privacy, sia per gli interessati. Egli è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti.

Per gli interessati e per l'autorità di controllo, egli rappresenta il punto di contatto. Gli interessati possono rivolgersi direttamente a lui per le questioni relative al trattamento. Così ancora il Garante della privacy può audirlo e chiedere informazioni circa il titolare che lo ha designato.

Il regolamento europeo stabilisce che i dati di contatto del DPO siano pubblicati e comunicati all'Autorità di controllo.

Il DPO ai sensi dell'art. 39 del Regolamento europeo deve:

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) 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.

9. Il registro delle attività di trattamento (artt. 30 del Regolamento europeo)

Il Regolamento europeo all'art. 30 stabilisce che ogni titolare e responsabile del trattamento debbano tenere e aggiornare un registro delle attività di trattamento, svolte sotto la propria responsabilità.

L'introduzione di questo nuovo obbligo discende dalla necessità di far mappare ai Titolari il patrimonio di dati che si detiene e le operazioni effettuate. Un efficace sistema di privacy si basa sulla tenuta e aggiornamento di un registro che consenta di svolgere nel tempo e in modo dinamico le ricognizioni e valutazioni, in termini di legittimità dei trattamenti e di adeguatezza delle misure di sicurezza adottate.

Il registro costituisce uno strumento operativo-gestionale di cui il titolare e il responsabile si avvalgono per assicurare il costante presidio sul patrimonio di dati personali che trattano. Esso è propedeutico allo svolgimento dell'analisi dei rischi sui trattamenti e alla individuazione delle misure di sicurezza più adeguate da adottare.

Il contenuto minimo del registro è definito all'art. 30 del Regolamento europeo, che al comma 4 stabilisce esso su richiesta del Garante della privacy vada messo a disposizione da parte del Titolare.

Con DUP 162 del 24 maggio 2018, è stato istituito ed approvato il registro delle attività di trattamento per il Consiglio regionale della Puglia, che va costantemente aggiornato, secondo quanto disposto dal citato provvedimento, tenuto conto di modifiche da apportare al trattamento o integrazioni che si rendesse necessario apportare o di nuovi trattamenti avviati non ricompresi nel registro.

10. La sicurezza dei dati – Indicazioni generali (art. 32 del Regolamento Europeo)

I dati personali, siano essi in formato digitale oppure su supporto cartaceo, devono essere custoditi con cura al fine di preservare le caratteristiche di **disponibilità, autenticità, integrità e riservatezza**.

Il Titolare deve preoccuparsi dell'adozione delle misure di sicurezza adeguate.

Il Considerando n. 39 specifica che: *"I dati personali dovrebbero essere trattati in modo da garantirne un'adeguata sicurezza e riservatezza, anche per impedire l'accesso o l'utilizzo non autorizzato dei dati personali e delle attrezzature impiegate per il trattamento."*

Il principio di "responsabilizzazione" ("accountability") impone di adottare (documentandone l'adozione) idonee misure tecniche e organizzative adeguate al rischio, per garantire la sicurezza dei trattamenti.

Le misure per la gestione del rischio sono di tipo tecnologico (cifatura, conservazione adeguata, anonimizzazione dei dati, minimizzazione, aggiornamenti servizi e software, test, controllo accessi e tracciamento operazioni) e di tipo organizzativo (policy di sicurezza logiche e fisiche, definizione di ruoli e della governance, istruzioni, formazione, procedure, audit).

L'articolo 32 del Regolamento europeo, elenca a titolo esemplificativo alcune misure:

"a) la pseudonimizzazione e la cifatura dei dati personali; b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento."

Ai sensi del Regolamento europeo e del Codice Privacy, non sussistono obblighi generalizzati di adozione di misure "minime" di sicurezza, diversamente da quanto previsto dalla previgente normativa nazionale (ex art. 33 del D. Lgs. n.196/2003, oggi abrogato). La valutazione circa le necessarie misure, di tipo tecnico e organizzativo, è rimessa al Titolare, il quale, caso per caso, le disporrà in rapporto ai rischi specificamente individuati per ciascuna categoria di trattamento. A tal fine risulta basilare che il Titolare svolga la preventiva attività, definita analisi dei rischi, di cui al paragrafo successivo.

Ciò che rileva è che le misure di sicurezza garantiscano un livello di sicurezza adeguato al rischio del trattamento (art. 32, paragrafo 1), che deve tener conto necessariamente di alcuni fattori: stato dell'arte e costi di attuazione, natura, oggetto, contesto e finalità del trattamento, probabilità dell'evento dannoso e gravità del danno conseguente.

11. L'analisi dei rischi (art. 32, par. 2, del Regolamento Europeo)

«Per “rischio” si intende uno scenario descrittivo di un evento e delle relative conseguenze, che sono stimate in termini di gravità e probabilità» per i diritti e le libertà.⁷

Il Regolamento europeo introduce il tema del rischio nel Considerando n. 75:

“I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare:

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

Il successivo Considerando n. 76 aggiunge: *“La probabilità e la gravità del rischio per i diritti e le libertà dell'interessato dovrebbero essere determinate con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento. Il rischio dovrebbe essere considerato in base a una valutazione oggettiva mediante cui si stabilisce se i trattamenti di dati comportano un rischio o un rischio elevato.”*

Gli elementi da considerare nella individuazione del rischio sono nel loro insieme: origine, natura, gravità, probabilità, impatto sui diritti e le libertà degli interessati.

Il rischio non si riferisce al titolare, ma al soggetto interessato. Si deve tener conto del fatto che i rischi possono variare nel corso del tempo, per cui la gestione del rischio è un “processo continuo”.

La valutazione del rischio deve riguardare:

- a. la sicurezza del trattamento
- b. gli effetti del trattamento.

Gli aspetti riguardanti la sicurezza del trattamento sono la **disponibilità del dato**, a fronte della sua distruzione, indisponibilità o perdita; l'**integrità** a fronte dell'alterazione, la **riservatezza** a fronte della divulgazione e di un accesso non autorizzato.

Gli effetti complessivi del trattamento da considerare sono, ad esempio, il danno per la reputazione, la discriminazione, il furto d'identità, perdite finanziarie, danni fisici o psicologici, la perdita di controllo dei dati, altri svantaggi economici o sociali, l'impossibilità di esercitare diritti, servizi o opportunità.

⁷ Cfr. “Linee guida del Gruppo di lavoro Articolo 29 , doc. WP248rev.1”

La valutazione del rischio – se i rischi sono elevati – può condurre ad effettuare anche una valutazione d'impatto (Protection Impact Assessment – PIA), espressamente prevista dall'art. 35 del Regolamento europeo.

12. La valutazione d'impatto (art. 35 del Regolamento europeo).

Il Considerando n. 84 così recita sulla valutazione d'impatto (nota anche come "Protection Impact Assessment" - PIA): *“Per potenziare il rispetto del presente regolamento qualora i trattamenti possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento dovrebbe essere responsabile dello svolgimento di una valutazione d'impatto sulla protezione dei dati per determinare, in particolare, l'origine, la natura, la particolarità e la gravità di tale rischio. L'esito della valutazione dovrebbe essere preso in considerazione nella determinazione delle opportune misure da adottare per dimostrare che il trattamento dei dati personali rispetta il presente regolamento. Laddove la valutazione d'impatto sulla protezione dei dati indichi che i trattamenti presentano un rischio elevato che il titolare del trattamento non può attenuare mediante misure opportune in termini di tecnologia disponibile e costi di attuazione, prima del trattamento si dovrebbe consultare l'autorità di controllo”.*

La valutazione d'impatto sulla protezione dei dati personali, secondo quanto previsto dall'art. 35 del Regolamento europeo, non è un istituto applicabile in ogni situazione. Lo stesso art. 35 configura la casistica interessata dalla PIA, caratterizzata dalla sussistenza di rischi elevati per i diritti e le libertà delle persone (si tratta quindi di un livello di rischio superiore al normale rischio insito nel trattamento di dati personali).⁸

Al comma 3 dell'art. 35, vengono poi esemplificati dei casi specifici in cui è richiesta la PIA, come ad esempio la sorveglianza su larga scala di zone accessibili al pubblico ovvero il trattamento su larga scala di categorie particolari di dati.

La PIA è, altresì, richiesta nei casi che saranno indicati dal Garante della privacy in un apposito elenco.

13. Databreach e registro dei databreach (art. 33 e 34 del Regolamento Europeo)

Nell'ipotesi di violazione di dati personali, il Titolare del trattamento deve notificare l'avvenuta violazione all'autorità di controllo competente senza ingiustificato ritardo (entro 72 ore). In tale notifica deve essere descritta nel dettaglio la natura della violazione, i dati dei titolari e dei responsabili del trattamento, le probabili conseguenze della violazione stessa e quali misure sono state o si intende adottare per farvi fronte (art. 33 del Reg. 679/16).

Quando la violazione comporta un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento, ai sensi dell'art 34, è obbligato a comunicare la violazione dei dati personali anche all'interessato.

⁸ il Garante della privacy ha messo a disposizione sul proprio sito un software per svolgere una valutazione d'impatto <https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment>.

Per altro verso, tale comunicazione non è necessaria se il titolare, che ha subito il databreach, ha messo preventivamente in atto misure di protezione tecnico-organizzative in grado di scongiurare il rischio per gli interessati (es. Dati personali pseudonimizzati) ovvero quando la comunicazione richiederebbe sforzi sproporzionati.

Si intendono oggetto dell'eventuale obbligo di notifica, anche i "data breach" avvenuti presso responsabili "esterni" o loro eventuali sub-responsabili (per quanto attiene ai trattamenti di dati effettuati da questi soggetti su delega).

L'art. 33, par.5, impone che il titolare del trattamento documenti qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. In detto registro vanno annotati anche gli incidenti occorsi presso i responsabili del trattamento eventuali sub-responsabili.

Il compito di istituire il registro di databreach è tipicamente proprio della struttura che si occupa di sicurezza informatica ed è alimentato, nei casi di sinistri, con il necessario ausilio e il supporto informativo delle strutture operative interessate dall'evento.

Tutte le persone autorizzate al trattamento devono essere adeguatamente istruite affinché trattino correttamente i dati personali e, con la massima celerità, informino il Titolare di ogni violazione rilevata, affinché quest'ultimo possa procedere con le suddette segnalazioni o registrazioni.

PARTE SECONDA

14. L'assetto organizzativo privacy del Consiglio regionale

Il Regolamento europeo richiede che il Consiglio Regionale riveda processi e ruoli aziendali, dotandosi di un nuovo **assetto organizzativo privacy**. In particolare il principio di *accountability* rende necessaria una corretta articolazione funzionale del ruolo del Titolare.

Gli adempimenti previsti dal Regolamento europeo in capo al titolare devono essere attribuiti, sulla base della normativa generale e dell'ordinamento specifico del Consiglio regionale della Puglia, alle strutture amministrative che hanno competenza a svolgere le attività da cui quegli adempimenti discendono.

Peraltro, a fronte di eventuali disfunzioni o non conformità nel trattamento di dati personali, sarebbe viziato da irragionevolezza attribuire genericamente la responsabilità al Consiglio regionale, in quanto Titolare, essendo l'azione dello stesso direttamente posta in essere dalle strutture amministrative.

Sul punto è utile ricordare che il Codice all'art. 2-quaterdecies riconosce al titolare il potere di prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la sua autorità.

Il Titolare quindi ha il potere di disegnare la propria organizzazione Privacy, attribuendo compiti e funzioni connessi al trattamento, rinvenibili in capo ad esso, a specifiche figure purché operanti sotto la sua autorità.

L'organigramma privacy del Consiglio Regionale della Puglia è raffigurabile come segue:

- **Titolare del trattamento (artt. 4, par. 7 e 24 del Regolamento europeo):** è la persona fisica o giuridica che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali. In detta funzione sono riassunti e ricompresi tutti i poteri e gli obblighi in capo al soggetto che per antonomasia è responsabile del trattamento dei dati personali. Il titolare è colui che risponde alla definizione ex lege. Ha un'investitura legale e ab origine. Solitamente nelle organizzazioni complesse le responsabilità (e connessi poteri) sono distribuite con delega, secondo il modello organizzativo prescelto. Per i trattamenti di dati personali effettuati dalle strutture amministrative del Consiglio regionale della Puglia, Titolare è il Consiglio, che ad ogni modo opera con deleghe e non trattiene a sé tutte le responsabilità.
- **Designato al trattamento:** è una figura introdotta nell'organizzazione privacy del Consiglio regionale della Puglia, che subentra alla figura del responsabile del trattamento ("interno") ex art. 29 del D. Lgs. n. 196/2003, oggi abrogato dal D.Lgs. n. 101/2018. Tenuto conto della complessità e della molteplicità delle funzioni istituzionali del Consiglio regionale della Puglia, in cui le scelte di gestione finanziaria, tecnica e amministrativa rientrano tra le specifiche competenze dei Dirigenti, il Titolare delega tutti i dirigenti in servizio presso il Consiglio Regionale della Puglia, ognuno per la parte di propria competenza, al trattamento di dati personali effettuato nello svolgimento dell'incarico ricevuto. I dirigenti in virtù delle proprie competenze istituzionali sono responsabili di attività delegate dal Titolare e rivestono il ruolo di Designati.

- **I responsabili del trattamento (art. 28 del Regolamento europeo):** sono soggetti esterni al Consiglio regionale della Puglia (ad. es. Società, consulenti, enti, ecc.) che nello svolgimento delle attività commissionate, trattano dati personali per conto del titolare, sulla base di un contratto che stabilisca gli elementi fondamentali del trattamento indicati all' art. 28 e che preveda anche quanto indicato agli artt. 30 e 33, par. 2, del Regolamento europeo. Essi devono essere selezionati dal titolare o dal designato, sulla base della loro capacità di garantire che nell'esercizio delle attività assegnate adottino di misure tecniche ed organizzative, tali da consentire che il trattamento soddisfi i requisiti del Regolamento europeo e assicuri la tutela dei diritti dell'interessato. Il Responsabile del trattamento, a differenza del Titolare, ha un'investitura negoziale che discende dalla sottoscrizione del contratto con il Titolare medesimo.
- **Sub-responsabili del trattamento (art. 28, par. 2, e art. 4 del Regolamento europeo):** i responsabili di cui alla lettera precedente (se previamente autorizzati per iscritto dal titolare o dal designato) possono affidare (con le stesse forme previste per il responsabile) lo svolgimento di specifiche attività di trattamento di dati personali a sub-responsabili. Tale avvalimento non li esime dal rispondere in solido per ogni eventuale trattamento illecito o non conforme al Regolamento europeo effettuato dai sub-responsabili.
- **Responsabile della protezione dei dati (artt. da 37 a 39 del Regolamento europeo):** con Deliberazione dell'Ufficio di Presidenza n. 159 de 21/06/2018, il ruolo di Responsabile della protezione dei dati ex art. 37 del Regolamento europeo per il Consiglio Regionale della Puglia, è stato assegnato alla Dirigente della Sezione Affari Istituzionali e Giuridici che ricopre anche per la Giunta Regionale detto incarico. La nomina del RPD, di cui il Regolamento europeo prevede si dia apposita diffusione, è oggetto di pubblicazione nel portale Amministrazione Trasparente del Consiglio regionale, (<http://trasparenza.consiglio.puglia.it/dettaglio/menu/4461/Responsabile-della-protezione-dei-dati>) ed è stata oggetto di specifica comunicazione al Garante della Privacy, ai sensi della normativa.
- **Persona autorizzata al trattamento dei dati (art. 29 del Regolamento europeo).** In detta categoria è ricompreso il personale del Consiglio regionale della Puglia che svolge attività che comporta trattamento di dati personali. Le persone fisiche che, operando sotto l'autorità del titolare del trattamento (o sotto l'autorità del Designato), effettuano operazioni di trattamento dei dati, devono necessariamente essere autorizzate dal Titolare (o dal Designato) e attenersi alle istruzioni dallo stesso ricevute. Le persone autorizzate al trattamento coincidono con gli "incaricati" del trattamento, previsti dal D.Lgs. 196/2003. Il Regolamento europeo non fa alcun riferimento alla necessità di «nominare» formalmente le persone autorizzate al trattamento. Ciò non vieta al titolare o al designato del trattamento, di nominarli, in modo da definire con maggiore chiarezza compiti e responsabilità, attraverso una specifica lettera di attribuzione d'incarico. Questa modalità operativa, già impiegata in attuazione del D. Lgs. n. 196/2003, costituisce una buona prassi funzionale all'attuazione del principio di accountability ed è opportuna per documentare la compliance al Regolamento europeo, rispetto a detto obbligo. In allegato alle presenti istruzioni, è disponibile un modello di autorizzazione del personale che potrà essere impiegato (e laddove opportuno o necessario anche integrato) dal Designato.
- **Referente privacy:** è la figura di cui, vista la specificità della materia, si suggerisce la presenza all'interno di ogni struttura del Consiglio. Essa è individuata dal Dirigente Designato e, presso la

struttura di appartenenza, coadiuva il designato e le persone autorizzate negli adempimenti in materia di privacy e supporta il designato nel coordinamento delle attività conseguenti.

- **Gruppo di lavoro regionale per la protezione dei dati personali:** costituito con Delibera di Giunta Regionale n. 794 del 2018, esso è coordinato dal RPD e composto dal Responsabile della transizione al digitale, dal dirigente della Sezione Risorse strumentali e tecnologiche del Dipartimento Salute, da un dirigente indicato dal Segretario Generale del Consiglio regionale della Puglia e da un rappresentante designato dalla società *in house* InnovaPuglia s.p.a., con la funzione di definire una policy comune a Consiglio e Giunta nella materia della protezione dei dati personali.

15. I compiti del Designato al trattamento

Il designato, nell'ambito delle proprie funzioni, al fine di poter fare fronte efficacemente alle diverse incombenze proprie del ruolo e di seguito indicate, si avvale della fattiva collaborazione dei Referenti privacy e delle persone autorizzate al trattamento, adeguatamente istruite e responsabilizzate sul tema.

Il designato, in particolare, deve:

- a) **Verificare la liceità del trattamento ai sensi dell'art. 6 ed il rispetto dei principi di cui all'art. 5.** Il Designato deve garantire nell'ambito della propria struttura e con riferimento ai trattamenti svolti da parte del personale della stessa, la compliance al Regolamento europeo, garantendo la tutela dei diritti dell'interessato. Particolare attenzione dovrà porre ai dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, dati genetici, biometrici, sulla salute e sulla vita sessuale nonché ai dati relativi a condanne penali e reati (artt. 9 e 10 del Regolamento europeo).
- b) **Introdurre**, conseguentemente alla verifica di cui sopra, **le necessarie modifiche al trattamento**, per renderlo conforme (se del caso) alla normativa e laddove ricorrano le condizioni disporre la cessazione dei trattamenti effettuati in violazione della medesima;
- c) **Essere accountability.** Il Designato deve documentare le scelte ad esso spettanti in materia di privacy, tenendo traccia – laddove possibile - della valutazioni e delle motivazioni che lo hanno condotto ad effettuare dette scelte.
- d) **Garantire la corretta informazione e l'esercizio dei diritti dell'interessato.** Il designato predispone le informative relativi al trattamento dei dati personali (art. 13 e 14 Reg.) e nelle fattispecie di cui agli articoli da 15 a 21 garantisce i diritti degli interessati, dando riscontro all'istante secondo quanto stabilito dall'art. 12.
- e) **Censire il patrimonio informativo.** Ogni designato e ogni persona autorizzata al trattamento devono conoscere ed essere consapevoli della natura e della tipologia dei dati personali trattati. La conoscenza di questi elementi è propedeutica a qualsiasi valutazione dei rischi sui dati trattati e alla conseguente individuazione delle contromisure da adottare. Il designato deve curare periodicamente il censimento delle Banche Dati e dei trattamenti di dati personali effettuati dalla struttura che dirige.
- f) **Adottare soluzioni di privacy design e privacy by default.** Il designato disegna processi e soluzioni applicative in cui si articola o che sono a supporto dell'attività di propria competenza, agendo per la

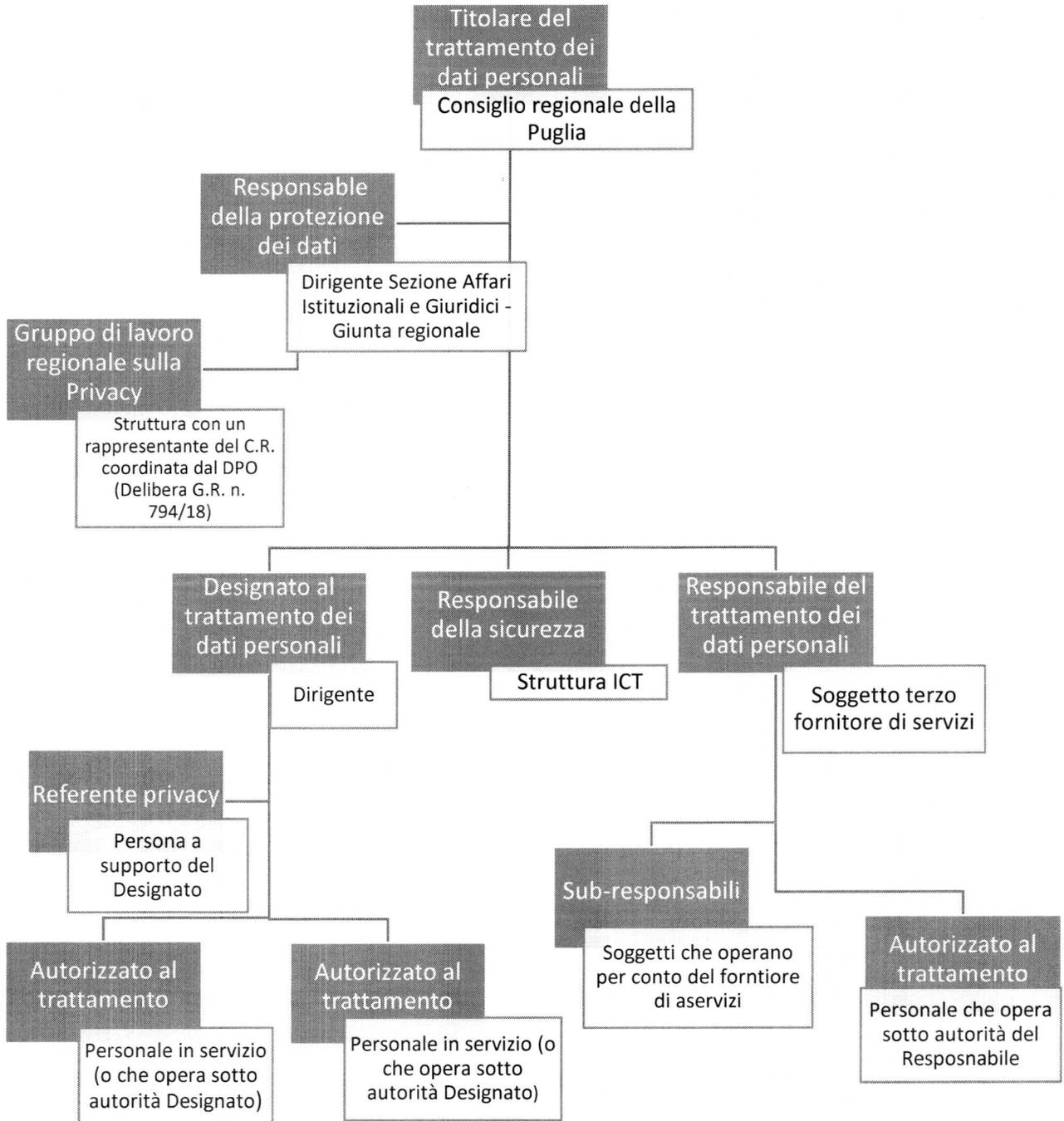
“protezione fin dalla progettazione” e per la “protezione per impostazione predefinita” dei dati personali che tratta.

- g) **Implementare il Registro** (unico) delle attività di trattamento istituito con DUP n. 162 del 2018 e pubblicato sotto Amministrazione Trasparente. Il registro delle attività di trattamento svolte per conto del titolare (art. 30, par. 2) è uno strumento fondamentale, avente lo scopo di disporre di un quadro aggiornato dei trattamenti dei dati in essere all'interno del Consiglio Regionale della Puglia. Esso va costantemente aggiornato, su richiesta del Designato al Segretario Generale, a seguito di nuovi trattamenti ovvero di modifiche sostanziali ai trattamenti già previsti. Il Registro contiene i dati di contatto del titolare, responsabile e DPO, finalità e categorie dei dati raccolti, descrizione delle misure tecniche e organizzative. Tale registro verrà messo a disposizione del Garante della privacy in caso di esplicita richiesta.
- h) **Collaborare con il Data Protection Officer** per consentire allo stesso lo svolgimento delle funzioni e dei compiti assegnati. Il Designato inoltre, sentito il Segretario Generale del Consiglio, dovrà coinvolgere tempestivamente e adeguatamente il DPO, in tutte le questioni rilevanti riguardanti la protezione dei dati personali della propria struttura.
- i) **Autorizzare al trattamento il personale e definire i profili di autorizzazione.** Il Designato deve individuare e autorizzare i soggetti incaricati di compiere specifiche operazioni di trattamento, fornendo agli stessi istruzioni per il corretto trattamento, sovrintendendo e vigilando sull'attuazione delle istruzioni impartite. Il designato dà disposizione e verifica che questi raccolgano e trattino dati personali strettamente indispensabili per lo svolgimento delle attività loro assegnate. Per i trattamenti effettuati con strumenti elettronici, il Designato individua l'ambito di trattamento cui corrisponde uno specifico “profilo di autorizzazione”. Egli incarica per iscritto all'occorrenza i soggetti cui affidare la custodia di particolari archivi o la tenuta delle credenziali di autenticazione tecniche o di accesso a specifici database. Il Designato autorizza al trattamento, anche eventuali collaboratori “esterni” (persone fisiche) del Consiglio, a prescindere dal rapporto contrattuale intrattenuto (ad es. stagisti, tirocinanti, ecc.), purché non dotati di potere decisionale autonomo (che li qualificerebbe più correttamente come responsabili). Nel conferire l'incarico e fornire le istruzioni, il designato può utilizzare il modello allegato (“nomina autorizzati al trattamento”), a corredo del presente documento, integrandolo con quanto ritenga necessario in considerazione delle caratteristiche dei trattamenti propri della struttura di riferimento.
- j) **Verificare costantemente la permanenza delle condizioni per la conservazione dei profili** di autorizzazione al trattamento dei dati personali, che dovranno essere revocate (a titolo esemplificativo) in caso di cessazione dal servizio, trasferimento di ufficio, assegnazione di diverse mansioni e compiti, risoluzione rapporto contrattuale, ecc.. Il Designato verifica costantemente la sussistenza delle condizioni per la conservazione dei profili di autorizzazione al trattamento dei dati personali, consentito ai singoli soggetti autorizzati, siano interni o esterni al Consiglio regionale.
- k) **Impartire istruzioni alla persona autorizzata affinché questa:** a) custodisca le proprie credenziali adoperandosi con la diligenza necessaria; b) non usi le credenziali altrui, di cui venisse accidentalmente a conoscenza; c) custodisca, nel caso di trattamenti cartacei, atti e documenti contenenti dati personali, con la cura necessaria, fino al completamento delle operazioni di trattamento; d) adotti, nel caso in cui i documenti contengano categorie particolari di dati personali, cautele e attenzioni ancora più stringenti a garantire che non accedano persone non autorizzate. Il modello di autorizzazione contiene un'indicazione più ampia e dettagliata delle accortezze necessarie da seguire durante le operazioni di trattamento.
- l) **Garantire la disponibilità dei dati in caso di prolungata assenza della persona autorizzata**, dando prescrizione organizzative (es: prevedendo la figura del custode della pw).

- m) **Regolamentare l'accesso negli archivi:** prevedendo apposite autorizzazioni per il personale autorizzato e la registrazione degli accessi con modalità cartacea, nel caso di accessi agli archivi non muniti di sistemi digitali di controllo accessi;
- n) **Contrattualizzare l'incarico di Responsabile "esterno".** Il designato nell'affidare ai sensi dell'art 28 ad un soggetto "esterno" al Consiglio (persona fisica o giuridica, pubblica o privata) attività che comportano un trattamento di dati personali, deve valutare che questo soggetto presenti *"garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del (...) regolamento"* e garantisca la tutela dei diritti dell'interessato. Il designato deve provvedere a formalizzare – mediante contratto – la nomina di responsabile ("esterno") del trattamento secondo quanto indicato nell'art. 28 del Regolamento europeo, prevedendo o meno la possibilità per il responsabile esterno di ricorrere a sub-responsabili e richiamando esplicitamente gli obblighi di cui agli artt. 30 e 33, par. 2, del Regolamento europeo.
- o) **Disciplinare il rapporto di contitolarità dei trattamenti.** Nell'ipotesi in cui si verta in fattispecie di contitolarità ossia di determinazione congiunta di finalità e mezzi da parte del Consiglio regionale della Puglia e uno o più soggetti diversi, autonomi titolari, il designato prima di avviare la relativa e sottostante attività determina mediante un accordo le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal Regolamento europeo, con riguardo particolare ai diritti dell'interessato ed alle informazioni di cui all'art. 13 e 14.
- p) **Garantire la sicurezza dei dati.** I dati personali, siano essi in formato digitale oppure su supporto cartaceo, devono essere custoditi con cura al fine di preservare le caratteristiche di disponibilità, autenticità, integrità e riservatezza. Il designato deve preoccuparsi, per quanto di competenza, dell'adozione delle misure di sicurezza adeguate e collaborare con la struttura competente in materia di sicurezza nello svolgimento dell'analisi dei rischi, anche nei casi di cui all'art. 35 e 36 del Regolamento europeo relativi alla valutazione di impatto ed alla consultazione preventiva. Il Designato valuterà per la parte di propria competenza, insieme al Responsabile della sicurezza, le misure necessarie ai sensi dell'art. 32, tenendo conto della tipologia di dati e di operazioni nonché di quanto stabilito dall'art. 32.
- q) **Gestire i Databreach:** nei casi di violazioni di dati personali avvenuti anche presso responsabili "esterni" o loro eventuali sub-responsabili (per quanto attiene ai trattamenti di dati affidati), il designato al trattamento deve effettuare una prima necessaria istruttoria. Valutati i rischi per i diritti e le libertà delle persone fisiche, dovrà avvisare tempestivamente la struttura competente in materia di sicurezza informatica, il titolare, il DPO, sentito il Segretario Generale, nonché implementare il registro dei databreach. Sussiste l'obbligo di notifica e comunicazione di avvenuta violazione dei dati personali sia al Garante della Privacy che, in determinati casi, anche ai diretti interessati spetta entro 72 ore dal sinistro (art. 33).
- r) **Individuare,** se ritiene opportuno, un **referente privacy** che lo supporti in tutte le attività a lui spettanti.

APPENDICE

Fig. 1



ELENCO TRATTAMENTI DATI PERSONALI DEL CONSIGLIO REGIONALE DELLA PUGLIA - REGISTRO EX ART. 30 REG.679/16 (D.U.P. 162/2018)

Segretariato Generale:

- Scheda n. 1 - Gestione del personale assegnato
- Scheda n. 2 - Valutazione del personale assegnato
- Scheda n. 3 - Protocollazione e gestione documentale
- Scheda n. 4 - Conservazione e tenuta dei documenti
- Scheda n. 5 - Gestione delle procedure di acquisizione di beni e servizi
- Scheda n. 6 - Gestione dei Provvedimenti dell'Ufficio di Presidenza, del Presidente del Consiglio regionale e delle determinazioni del Segretario generale e dei dirigenti
- Scheda n. 7 - Controllo accessi all'aula consiliare
- Scheda n. 8 - Cerimoniale
- Scheda n. 9 - Concessione di contributi a enti o organismi senza scopo di lucro
- Scheda n. 10 - Concessione di patrocini a enti o organismi senza scopo di lucro
- Scheda n. 11 - Assistenza all'Ufficio di Presidenza nel procedimento di riesame del provvedimento di diniego di accesso agli atti
- Scheda n. 12 - Formazione e tenuta albo candidati e procedura di selezione dei revisori dei conti

Sezione Assemblea e Commissioni consiliari permanenti:

- Scheda n. 1 - Valutazione del personale
- Scheda n. 2 - Gestione del personale assegnato
- Scheda n. 3 - Conservazione e tenuta dei documenti
- Scheda n. 4 - Documentazione dell'attività istituzionale delle Commissioni permanenti, speciali d'indagine o d'inchiesta
- Scheda n. 5 - Documentazione e pubblicità dell'attività istituzionale dell'Assemblea consiliare
- Scheda n. 6 - Convocazione di sedute e audizioni delle Commissioni consiliari, comunicazioni e invio di documentazione
- Scheda n. 7 - Attività politica di indirizzo e controllo – sindacato ispettivo
- Scheda n. 8 - Gestione delle presenze dei Consiglieri regionali alle sedute del Consiglio regionale e delle Commissioni
- Scheda n. 9 - Anagrafe dei titolari di cariche elettive
- Scheda n. 10 - Nomine e designazioni di competenza del Consiglio regionale
- Scheda n. 11 - Protocollazione e gestione documentale
- Scheda n. 12 - Acquisti di beni e servizi e gestione dei rapporti contrattuali

Sezione Studio e Documentazione a supporto dell'attività legislativa:

- Scheda n. 1 - Gestione del personale assegnato
- Scheda n. 2 - Rapporti di collaborazione e affidamento di incarichi di consulenza, studio e ricerca
- Scheda n. 3 - Protocollazione e gestione documentale
- Scheda n. 4 - Valutazione del personale
- Scheda n. 5 - Conservazione e tenuta dei documenti
- Scheda n. 6 - Formazione professionale del personale e tirocini formativi

Sezione Affari e Studi giuridici e legislativi:

- Scheda n. 1 - Gestione del personale assegnato
- Scheda n. 2 - Protocollazione e gestione documentale
- Scheda n. 3 - Valutazione del personale assegnato
- Scheda n. 4 - Istruttoria, elaborazione adozione atti dirigenziali di impegno e di spesa
- Scheda n. 5 - Conservazione e tenuta dei documenti
- Scheda n. 6 - Elaborazione parere per l'Ufficio di Presidenza in materia di ricorsi avverso diniego accesso agli atti

- Scheda n. 7 - Strumenti di democrazia diretta - iniziativa popolare – referendum

Sezione Amministrazione e Contabilità:

- Scheda n. 1 - Rapporti contrattuali con fornitori di beni e servizi
- Scheda n. 2 - Gestione del fondo economale di cassa e rendiconto
- Scheda n. 3 - Acquisizione di beni e servizi tramite fondo economale
- Scheda n. 4 - Gestione dei rapporti con fornitori e liquidazione delle relative spese
- Scheda n. 5 - Analisi e applicazione delle procedure contabili, dalla liquidazione della spesa all'emissione del mandato di pagamento
- Scheda n. 6 - Adempimenti amministrativo-contabili riguardanti il trattamento economico, diretto ed indiretto, Consiglieri regionali
- Scheda n. 7 - Gestione delle procedure di acquisizione di beni e servizi
- Scheda n. 8 - Gestione economica, fiscale e previdenziale delle indennità dei consiglieri e assessori regionali, dei componenti del CORECOM, e dei Garanti
- Scheda n. 9 - Gestione mandati di pagamento e reversali di incasso
- Scheda n. 10 - Protocollazione e gestione documentale
- Scheda n. 11 - Conservazione e tenuta dei documenti
- Scheda n. 12 - Valutazione del personale
- Scheda n. 13 - Adempimenti amministrativo-contabili per la liquidazione dei compensi dei collaboratori con rapporto di lavoro coordinato e continuativo
- Scheda n. 14 - Gestione del personale assegnato

Sezione Risorse Umane:

- Scheda n. 1 - Gestione del personale assegnato
- Scheda n. 2 - Rapporti contrattuali con fornitori di servizi, affidamento di incarichi di consulenza, gestione dei rapporti e liquidazione delle relative spese
- Scheda n. 3 - Gestione del rapporto di lavoro
- Scheda n. 4 - Reclutamento ed instaurazione del rapporto di lavoro
- Scheda n. 5 - Protocollazione e gestione documentale
- Scheda n. 6 - Conservazione e tenuta dei documenti
- Scheda n. 7 - Valutazione del personale
- Scheda n. 8 - Formazione professionale del personale e tirocini formativi
- Scheda n. 9 - Adempimenti amministrativo-contabili per la liquidazione del trattamento economico del personale consiliare e dei compensi dei collaboratori con rapporto di lavoro coordinato e continuativo

Sezione Informatica e Tecnica:

- Scheda n. 1 - Gestione del personale assegnato
- Scheda n. 2 - Rapporti contrattuali con fornitori di beni e servizi
- Scheda n. 3 - Gestione della strumentazione e della rete informatica ed attuazione delle politiche di sicurezza informatica
- Scheda n. 4 - Utenza telefonia mobile
- Scheda n. 5 - Gestione assegnazione caselle PEC
- Scheda n. 6 - Gestione Firma Digitale
- Scheda n. 7 - Protocollazione e gestione documentale
- Scheda n. 8 - Conservazione e tenuta dei documenti
- Scheda n. 9 - Valutazione del personale

Sezione Biblioteca e comunicazione istituzionale:

- Scheda n. 1 - Gestione del personale assegnato
- Scheda n. 2 - Conservazione e tenuta dei documenti
- Scheda n. 3 - Protocollazione e gestione documentale
- Scheda n. 4 - Valutazione del personale
- Scheda n. 5 - Gestione delle procedure di acquisizione di beni e servizi
- Scheda n. 6 - Schede utenti e mailing list della biblioteca consiliare

- Scheda n. 7 - Gestione del portale istituzionale del Consiglio regionale
- Scheda n. 8 - Infopoint del Consiglio Regionale della Puglia
- Scheda n. 9 - Visite formative finalizzate alla conoscenza dell'istituzione consiliare
- Scheda n. 10 - Organizzazione di eventi e iniziative rivolte al pubblico
- Scheda n.11 - Gestione delle comunicazioni degli utenti dei social network

Sezione Garanti Regionali:

- Scheda n. 1 - Gestione del personale assegnato
- Scheda n. 2 - Protocollazione e gestione documentale
- Scheda n. 3 - Conservazione e tenuta dei documenti
- Scheda n. 4 - Valutazione del personale
- Scheda n. 5 - Rapporti contrattuali con fornitori di beni e servizi
- Scheda n. 6 - Concessione di patrocini e contributi a enti o organismi del terzo e quarto settore
- Scheda n. 7 - Gestione portale web e newsletter
- Scheda n. 8 - Redazione comunicati stampa e rapporti con ufficio stampa del consiglio regionale/ giunta regionale
- Scheda n. 9 - Gestione segnalazioni
- Scheda n. 10 - Tenuta registro organizzazioni terzo e quarto settore
- Scheda n. 11 - Gestione elenco tutori legali volontari

Sezione Stampa:

- Scheda n. 1 - Gestione del personale
- Scheda n. 2 - Gestione delle procedure di acquisizione di beni e servizi
- Scheda n. 3 - Gestione della mailing list dei giornalisti esterni
- Scheda n. 4 - Valutazione del personale
- Scheda n. 5 - Conservazione e tenuta dei documenti
- Scheda n. 6 - Protocollazione e gestione documentale

Comitato Regionale Per Le Comunicazioni – CORECOM:

- Scheda n. 1 - Conciliazioni e definizioni delle controversie tra utenti e operatori delle comunicazioni elettroniche
- Scheda n. 2 - Gestione del portale web del Corecom Puglia
- Scheda n. 3 - Esercizio delle funzioni di garanzia e di vigilanza e controllo in tema di comunicazioni, anche delegate ai CORECOM da parte dell'Autorità garante, ai sensi dell'art. 1, comma 13 della legge 249/1997; Trasmissioni dell'accesso radio-televisivo (L. 103/1975); Erogazione dei contributi alle emittenti locali (D.M. 292/2004)
- Scheda n. 4 - Protocollazione e gestione documentale per l'area organizzativa omogenea Corecom
- Scheda n. 5 - Gestione del personale assegnato
- Scheda n. 6 - Rapporti contrattuali con fornitori di beni e servizi
- Scheda n. 7 - Valutazione del personale
- Scheda n. 8 - Conservazione e tenuta dei documenti

ALLEGATO A.1

Modello di autorizzazione al trattamento dei dati personali

AUTORIZZAZIONE E ISTRUZIONI PER IL TRATTAMENTO

DEI DATI PERSONALI

EX ART. 29 DEL REGOLAMENTO (UE) N. 2016/679

Il Sottoscritto/la sottoscritta [•], Dirigente della struttura [•], del Consiglio regionale della Puglia, in qualità di Designato al trattamento dei dati personali, per conto del Consiglio regionale, Titolare del trattamento, giusta Delibera dell'Ufficio di Presidenza n. [•] avente ad oggetto "*Protezione dei dati personali di Titolarità del Consiglio regionale. Attribuzione di funzioni e compiti a soggetti designati e istruzioni ai soggetti ai soggetti autorizzati, ai sensi dell'art. 2-quaterdecies del D.Lgs. 196/2003*", visto il Regolamento (UE) n. 2016/679 recante il "Regolamento Generale sulla Protezione dei Dati personali", visto il D.lgs. 196/2003 recante "Codice in materia di protezione dei dati personali", come modificato dal D.Lgs. 101/2018, e richiamato quanto disposto dalla Deliberazione dell'Ufficio di Presidenza n. [•],

AUTORIZZA

il/la sig/sig.ra [•] in servizio presso [•] del Consiglio regionale della Puglia con contratto di lavoro [•] (di seguito anche "Autorizzato"), con riferimento alle mansioni, compiti e attività affidati per l'esecuzione degli obblighi discendenti dal rapporto contrattuale con l'Amministrazione, a trattare i dati personali necessari per lo svolgimento della propria attività lavorativa e a eseguire le conseguenti operazioni di trattamento, anche mediante strumenti elettronici, con riferimento ai trattamenti della scheda n. [•] del Registro dei trattamenti di dati personali del Consiglio regionale (*cf. DUP 162/2018 ed elenco contenuto nel documento "Compiti e istruzioni per il designato al trattamento dei dati personali ai sensi dell'art. 2-quaterdecies del D.Lgs. 196/03"*).

In qualità di Autorizzato al trattamento, Ella deve attenersi scrupolosamente alle istruzioni di seguito fornite nonché a quelle contenute anche in altri documenti di policy che dispongano in relazione a profili rilevanti per la privacy e la sicurezza (es: manuali operativi e regolamenti interni del Consiglio).

Il mancato rispetto da parte dell'Autorizzato delle istruzioni impartite dall'Amministrazione e degli obblighi connessi all'autorizzazione al trattamento potrà costituire causa di responsabilità disciplinare, fermi restando gli altri profili di responsabilità amministrativa, civile e penale in caso di illecito trattamento dei dati personali.

Si richiamano i principali atti normativi che disciplinano il trattamento dei dati personali a cui l'Autorizzato deve richiamarsi: Reg. 679/2016; D. Lgs. 196/2003; Deliberazione Garante protezione dei dati personali n. 243/14 (G.U. n. 134/2014).

Le istruzioni che con il presente atto si forniscono vanno lette congiuntamente al documento "Compiti e istruzioni per il Designato al trattamento dei dati personali" (Allegato A – Compiti e Istruzioni per il Designato al trattamento).

La presenta autorizzazione sostituisce le precedenti nomine di incaricato al trattamento e non costituisce incarico ulteriore, costituendo una prescrizione sulla modalità con cui svolgere l'ordinaria attività assegnatale.

ISTRUZIONI SULLE MODALITÀ DI TRATTAMENTO DEI DATI PERSONALI

L'autorizzato al trattamento deve:

- 1) Raccogliere e trattare i dati, in formato analogico e/o digitale, esclusivamente al fine di adempiere alle obbligazioni contrattuali discendenti dal rapporto di lavoro/collaborazione con l'Amministrazione regionale e per i trattamenti per i quali si è autorizzato;
- 2) Trattare i dati di cui si viene a conoscenza, operando in modo lecito e secondo correttezza, nel rispetto di quanto stabilito dalla normativa vigente, verificando la liceità del trattamento (art. 6 del Reg. 679/16, artt. 2-ter, 2-sexies 2-octies del D.Lgs 196/2003) e il rispetto dei principi stabiliti (art. 5 del reg. 679/16);
- 3) Richiedere e raccogliere dagli interessati nonché trattare i dati strettamente necessari e indispensabili per lo svolgimento delle attività assegnate, in ottemperanza al principio di minimizzazione dei dati, verificando anche nel corso del trattamento che gli stessi siano pertinenti e non eccedenti rispetto alla finalità del trattamento;
- 4) Verificare, per quanto di competenza, l'esattezza, la completezza e l'aggiornamento dei dati, provvedendo, nel caso, alla rettifica degli stessi;
- 5) Consultare e, per quanto di sua competenza, proporre al Designato l'aggiornamento del Registro delle attività di trattamento istituito con DUP n. 162 del 2018;
- 6) Fornire agli interessati al momento della raccolta del dato le informazioni ex art. 13 del Reg.679/16, utilizzando il modello allegato alla presente (allegato A2- INFORMATIVA);
- 7) Fornire agli interessati le informazioni di cui all'art. 14 del Reg. 679/16, nel caso di informazioni non raccolte presso l'interessato, utilizzando il modello allegato alla presente (allegato A2 - INFORMATIVA);
- 8) Garantire la riservatezza del dato e non comunicarlo a colleghi o terzi;
- 9) Dare comunicazione o diffusione dello stesso, solo nei casi previsti dalla legge o dal regolamento. Attenzione: attenersi scrupolosamente alle regole sulla comunicazione e diffusione dei dati, stabilite all'art. 2-ter, 2-sexies e 2-opties. In linea generale si ricorda che la comunicazione è ammessa nei casi previsti dalla legge o da regolamento o previo parere positivo dell'Autorità Garante. La diffusione è ammessa nei soli casi previsti da legge. Non è ammessa in alcun caso la diffusione di dati relativi allo stato di salute. Si rinvia a quanto contenuto nelle istruzioni per il Designato nell'allegato A).
- 10) Redigere atti e documenti oggetto di pubblicazione, tenendo conto delle "Linee Guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati", adottate dal Garante con Del. N. 243/14 e pubblicate in GU n. 134 del 12.6.2014. Attenzione: in linea generale l'interessato va reso identificabile solo nel caso in cui ciò sia previsto da una norma di legge o regolamento ovvero, quando il trattamento riguarda dati "sensibili" o "giudiziari", se ciò sia strettamente indispensabile per il raggiungimento della finalità per cui è prevista la pubblicazione. In tali fattispecie, nella redazione di provvedimenti, atti e documenti, i nomi e i cognomi identificativi delle persone fisiche devono comparire per non più di una volta. Essi devono essere sostituiti nel corpo del testo da espressioni quali, a seconda dei casi, "il destinatario del provvedimento", "l'interessato", "il controinteressato", "il beneficiario" e simili.
- 11) Osservare gli obblighi di riservatezza anche successivamente alla cessazione del rapporto di lavoro;

- 12) Non effettuare copie analogiche o digitali di dati, archivi e banche dati contenenti dati personali, se non applicando un principio di stretta necessità (ad es: ai fini di garantire la disponibilità del dato) e comunque solo per lo svolgimento dell'attività lavorativa;
- 13) Accedere esclusivamente agli archivi e alle banche dati per cui si sia stati autorizzati;
- 14) Custodire i fascicoli in modo da evitare che terzi o colleghi non autorizzati possano accedervi, ad esempio non lasciandoli incustoditi sulla scrivania. Maggiore attenzione e precauzione è richiesta per i fascicoli contenenti dati "sensibili" (art. 9 del Reg. 679/16) e "giudiziari" (art.10 del Reg. 679/16), da deporre dopo l'uso in armadi o cassetti chiusi a chiave;
- 15) Non comunicare a terzi o colleghi e custodire con cura e diligenza le credenziali per l'accesso e l'utilizzo degli strumenti elettronici con cui sono trattati i dati personali (es: non impiegare post-it con trascritta pw facilmente reperibili);
- 16) Collaborare con il Designato al trattamento affinché, nei casi di prolungata assenza, siano attivate le misure organizzative che consentono di accedere agli strumenti elettronici in uso (es: accesso con i privilegi di amministratore di sistema; accesso straordinario del Designato o collega incaricato);
- 17) Bloccare le sessioni di lavoro (con il comando CTRL ALT CANC e azionando il tasto INVIO) ogniqualvolta ci si allontana dalla propria workstation (postazione di lavoro);
- 18) Modificare la pw rendendola complessa ed evitando parole che possano essere associate all'utente con semplicità;
- 19) Evitare di lasciare in luoghi accessibili a terzi (stanze con stampanti di rete) copie di documenti contenenti dati personali;
- 20) Qualora sia necessario distruggere documenti contenenti dati personali (ad esempio perché stampati per errore), assicurarsi che siano distrutti in modo da non essere recuperati;
- 21) Consultare ed applicare per quanto di competenza il documento "Compiti e istruzioni per il Designato al trattamento dei dati personali", allegato alla presente (allegato A).
- 22) Segnalare tempestivamente al Designato al trattamento situazioni di rischio per la sicurezza dei dati di cui si sia venuti a conoscenza o eventi che si ritiene possano comportare la violazione di dati personali;
- 23) Nell'ipotesi di incertezza sulle modalità del trattamento dei dati, chiedere informazioni e indicazioni al Dirigente Designato.

Il Dirigente Designato al Trattamento

Io sottoscritto/a [•] dichiaro di aver letto il documento (composto di n. 3 pagine), di aver compreso le istruzioni sopra riportate sulle modalità di trattamento da seguire in qualità di autorizzato ex art. 29 del Regolamento (UE) n. 2016/679 e di averne ricevuto copia.

Data _____

L'Autorizzato

ALLEGATO A.2

INFORMAZIONI AI SENSI DELL'ART. 13 [o 14 (specificare)] DEL REGOLAMENTO UE 2016/679.

Gentilissimo/a,

ai sensi dell'art. 13 e (in alternativa 14) del Regolamento UE n.679 del 2016 desidero informarLa che il trattamento dei Suoi dati personali sarà improntato ai principi di correttezza, liceità e trasparenza e di tutela della Sua riservatezza e dei Suoi diritti.

Pertanto, Le fornisco le seguenti informazioni:

Titolare, Designato e Responsabile della protezione dei dati

Il Titolare del trattamento dei dati è il Consiglio regionale della Puglia, con sede in Via Capruzzi, n. 204, tel. +39 080.5402772, protocollo@pec.consiglio.puglia.it, che ha delegato per lo specifico trattamento in oggetto il/la Dirigente [•] (indicare Sezione/Servizio), Pec [•]

Il Responsabile della protezione dei dati del Consiglio regionale della Puglia è l'Avv. Silvia Piemonte, nominata con Deliberazione dell'Ufficio di Presidenza n. 159 del 24/05/2018.

Pec: sezaffariistituzionaligiuridici@pec.rupar.puglia.it, tel. 080.540.6925.

Finalità del trattamento dei dati e base giuridica

Il trattamento è finalizzato a [•] (specificare la finalità). Tale finalità è riconducibile alle disposizioni relative al trattamento di cui all'art... (specificare, se possibile, la norma che individua la finalità. Nel caso in cui il trattamento riguardi dati ex art. 9 e 10 del Reg. 679/16, si consiglia di consultare preventivamente le materia indicate in elenco agli artt. 2-sexies e 2-octies del D.Lgs. 196/2003, come modificato dal D.Lgs. 101/2018).

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 ai sensi dell'art. 6, par. 1, lett. e), del Reg. UE 679/2016.

La base giuridica del trattamento è [•] (indicare la norma)

(in alternativa) Il trattamento è necessario per adempiere un obbligo legale al quale il Consiglio regionale della Puglia è soggetto (indicare la norma che prevede l'obbligo).

Destinatari e categorie di destinatari dei dati e trasferimento dei dati.

I Suoi dati sono trattati dal personale della struttura appositamente autorizzato che opera sotto l'Autorità del Titolare, ai sensi dell'art. 2-quaterdecies del D.Lgs. 196/2003, come modificato dal D.Lgs. 101/2018.

(Se applicabile) I Suoi dati sono trattati altresì dal Responsabile del trattamento ex art. 28, [•] (dati identificativi/denominazione sociale).

(Se applicabile) I suoi dati possono essere comunicati, anche per via telematica, ai seguenti destinatari o categorie di destinatari [•] (sarebbe opportuno indicare la base normativa della comunicazione, anche se l'art. 13 del Reg. 679/16 non lo prevede espressamente. Ad ogni modo verificare che essa sia lecita comunicazione, ai sensi di quanto stabilito dagli artt. 2-ter, 2-sexies e 2-octies del D.Lgs. 196/2003, come modificato dal D.Lgs. 101/2018).

I Suoi dati saranno/non saranno oggetto di diffusione (*sarebbe opportuno indicare la base normativa della comunicazione, anche se l'art. 13 del Reg. 679/16 non lo prevede espressamente. Ad ogni modo verificare preventivamente che la comunicazione sia lecita, ai sensi di quanto stabilito dagli artt. 2-ter, 2-sexies e 2-octies del D.Lgs. 196/2003, come modificato dal D.Lgs. 101/2018*

I Suoi dati saranno trattati all'interno dell'Unione Europea e conservati su server ubicati all'interno dell'Unione Europea (*in caso contrario, specificare quanto previsto dall'art. 13, par. 1, lett. f).*

Modalità del trattamento e conservazione dei dati

Il trattamento sarà svolto in forma automatizzata e/o manuale, nel rispetto di quanto previsto dall'art. 32 del Reg. UE 679/2016, ad opera di soggetti appositamente autorizzati e in ottemperanza a quanto previsto dall'art. 29 del Reg. UE 679/2016 e dall'art. 2-quaterdecies del D.Lgs. 196/2003.

Le segnalo che, nel rispetto dei principi di liceità, limitazione delle finalità e minimizzazione dei dati, ai sensi dell'art. 5 del Reg. UE 679/2016, i Suoi dati personali saranno conservati per il periodo di tempo necessario per il conseguimento delle finalità per le quali sono raccolti e trattati

(trattasi di una previsione di carattere generale. Verificare la pertinenza e corrispondenza al trattamento cui l'informativa si riferisce).

Conferimento dei dati

Il conferimento dei dati per le finalità sopra indicate è facoltativo/obbligatorio. L'eventuale Suo rifiuto comporta [•] (*es: l'impossibilità di ...*)

Diritti dell'interessato

In relazione ai dati personali da Lei forniti, ferme restando le condizioni ed i limiti stabiliti dal Reg. 679/16 e dal D.Lgs. 196/2003, Lei ha il diritto di accedere ai dati personali ed alle informazioni contenute (art. 15 del Reg. UE 679/2016), di chiedere la rettifica (art. 16 del Reg. UE 679/2016), di richiedere la cancellazione (Art.17 del Reg. UE 679/2016), di ottenere la limitazione del trattamento (art. 18 del Reg. UE 679/2016), di opporsi al trattamento (art. 21 del Reg. UE 679/2016) e di proporre reclamo (art. 77 del Reg. UE 679/2016).

[(Nel caso di informazioni non raccolte presso l'interessato, l'informativa va integrata con queste informazioni di cui all'art. 14 del Reg. 679/16:)]

Categoria di dati trattati

Indicare i dati o le categorie di dati, con riferimento a quelli individuati agli artt. 9 e 10 del Reg. 679/16 [•]

Fonte da cui hanno origine i dati

[•] (*Specificare se la fonte è accessibile al pubblico.*)

Per il Consiglio regionale della Puglia - Titolare

Il/La Dirigente della _____

(Firma) _____

Io/la sottoscritto/a _____

dichiaro di aver preso visione della presente informativa

(Data) _____

(Firma) _____