REGIONE PUGLIA

SEGRETERIA GENERALE DEL PRESIDENTE

SEZIONE AFFARI ISTITUZIONALI E GIURIDICI

PROPOSTA DI DELIBERAZIONE DELLA GIUNTA REGIONALE

Codice CIFRA: AIG/DEL/2017/00003

OGGETTO: Adozione modelli omogenei per la designazione delle Società in house (InnovaPuglia S.p.A. – Puglia Sviluppo S.p.A.) quali Responsabili esterni del Trattamento di dati personali ai sensi del D.Lgs 196/2003 e tenendo conto di quanto disposto con il Reg. UE 2016/679.

Il Presidente della Giunta Regionale sulla base dell'istruttoria espletata dal Dirigente della Sezione Affari Istituzionali e Giuridici e, confermata dal Segretario Generale del Presidente della Giunta regionale, anche in qualità di Responsabile dell'Anticorruzione e Trasparenza, riferisce quanto segue:

Premesso che

- Con DGR n.1518 del 31.7.2015 è stato adottato l'Atto di Alta Organizzazione del modello organizzativo denominato "Modello Ambidestro per l'Innovazione della macchina Amministrativa regionale MAIA";
- Con DPGR n. 304 del 10 maggio 2016 sono state adottate modifiche ed integrazioni al decreto del 31 luglio 2015, n. 443 di adozione del modello organizzativo denominato "Modello Ambidestro per l'innovazione della macchina Amministrativa regionale" MAIA";
- Con DPGR n. 316 del 17 maggio 2016 sono state definite le Sezioni di Dipartimento e le relative funzioni in attuazione del modello MAIA di cui al Decreto del Presidente della Giunta Regionale 31 luglio 2015 n. 443.
- DGR n. 2043 del 16 novembre 2015, è stato nominato il Responsabile della Trasparenza e Prevenzione della Corruzione in capo al Segretario Generale della Presidenza (art.7. comma 1 Legge n. 190/2012 e art. 43, comma 1, D.Lgs. n. 33/2013);
- DGR n. 2063 del 21.12.2016 Adempimenti ai sensi del D. Lgs. n. 196/2003 "Codice in materia di protezione dei dati personali. Designazione dei Responsabili del Trattamento di dati personali in base al nuovo modello organizzativo MAIA" sono stati nominati i Responsabili del trattamento dati all'interno della Regione.

Rilevato che

- Il D. Lgs. 196/2003 "*Codice in materia di protezione dei dati personali*" impone all'Amministrazione regionale una serie di obblighi a tutela dei dati personali trattati e detenuti per lo svolgimento dei propri compiti e attività istituzionali;
- Con il Reg. reg. n. 5 del 25 maggio 2006 la Regione Puglia ha individuato le attività il cui svolgimento comporta il trattamento di dati sensibili e giudiziari;
- Con delibera n. 243 del 15 maggio 2014 il Garante per la protezione dei dati personali ha definito 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" (Pubblicato sulla Gazzetta Ufficiale n. 134 del 12 giugno 2014);
- Il Regolamento (UE) 2016/679 ha introdotto nuovi adempimenti relativi alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati;
- La Direttiva (UE) 2016/680 regola i trattamenti di dati personali nei settori di prevenzione, contrasto e repressione dei crimini pubblicati il 4 maggio 2016 sulla Gazzetta Ufficiale dell'Unione Europea (GUUE);
- Nelle more dell'adozione dei Decreti delegati di cui all'art. 13 della L. 25 ottobre 2017 n. 163.

Considerato che

- L'art. 2 del D.Lgs. n. 196/2003 recita che "il trattamento dei dati personali è disciplinato assicurando un elevato livello di tutela dei diritti e delle libertà … nel rispetto dei principi di semplificazione…".
- Quando il trattamento dei dati è effettuato da una pubblica Amministrazione, ai sensi dell'art. 28 del D.Lgs. n. 196/2003, titolare del trattamento è l'entità nel suo complesso, ossia la Regione Puglia.
- Nella Regione Puglia in base ai poteri assegnati agli organi statutari il "Titolare del trattamento" è la Giunta regionale laddove alla stessa competano le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza dei dati.
- L'art. 24 del Regolamento (UE) 2016/679 dispone che il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al regolamento; tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.
- Il Titolo IV del succitato D.lgs. n. 196/2003 prevede (articoli 29 e 30) altresì la facoltà per il Titolare di designare i Responsabili e gli Incaricati del trattamento ai quali sono attribuiti funzioni, compiti, poteri e responsabilità differenti.
- L'art. 28 del Regolamento (UE) 2016/679 dispone che il Titolare ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative

adeguate in modo tale che il trattamento soddisfi i requisiti del regolamento e garantisca la tutela dei diritti dell'interessato.

- L'allegato alla Dgr. 2063 del 2017 prevede che possano essere nominati Responsabili esterni nei casi in cui l'Amministrazione regionale affidi ad un soggetto esterno (persona fisica o giuridica, pubblica o privata) operazioni di trattamento che presuppongono l'esercizio di un potere decisionale accanto a quello del Responsabile del trattamento.
- Il Responsabile, preposto al trattamento di dati personali, deve essere individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia sufficienti per mettere in atto misure tecniche e organizzative adeguate del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza e, dunque, egli deve essere in grado di agire con sufficiente autonomia gestionale, pur nell'ambito degli incarichi e delle competenze assegnatigli dal Titolare e nel rispetto delle prescrizioni impartite dallo stesso.
- Le società in house InnovaPuglia e Puglia Sviluppo possono ricoprire il ruolo di contitolare del trattamento o di responsabile "esterno", per lo svolgimento delle attività assegnate dalla Regione Puglia.
- Nel caso in cui le società in house ricoprano il ruolo di responsabile del trattamento il referente per le attività assegnate (Dirigente di Sezione o Direttore di Dipartimento), in qualità di responsabile del trattamento, deve provvedere ad implementare o specificare le misure tecniche ed organizzative previste nell'allegato A del presente documento, a seconda della tipologia e delle modalità di trattamento, da eseguire per svolgere lo specifico affidamento, utilizzando come schema di riferimento l'allegato B.
- Qualora siano presenti specifiche e peculiari esigenze, tale individuazione non è effettuata e quindi i soggetti esterni non sono responsabili del trattamento di dati personali, ma titolari o contitolari dello stesso. Il referente per le attività assegnate (Dirigente di Sezione o Direttore di Dipartimento) in accordo con il Responsabile della protezione dati (Data Protection Officer) della Società in house deve provvedere a redigere in nome e per conto del titolare del trattamento un accordo, nel quale devono essere definiti le rispettive responsabilità, ruoli e i rapporti dei contitolari con gli interessati in merito all'osservanza degli obblighi normativa da rispettare per il trattamento dei dati, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni sul trattamento sono soggetti. Nell'accordo si deve designare un punto di contatto per gli interessati.

Considerato inoltre che:

- la Società in house InnovaPuglia in base allo Statuto svolge i seguenti compiti: supporto tecnico alla PA regionale per la definizione, realizzazione e gestione di progetti di innovazione basati sulle ICT per la PA regionale, nonché supporto alla programmazione strategica regionale a sostegno dell'innovazione. In questo ambito, le attività caratteristiche della Società sono:

  • lo svolgimento di compiti di centrale unica di committenza e/o di stazione unica appaltante;
  • la gestione di banche dati strategiche anche per il conseguimento di obiettivi economico-finanziari;
  • lo sviluppo, la realizzazione, la conduzione e la gestione delle componenti del sistema informativo regionale e di infrastrutture pubbliche di servizio della Società dell'Informazione;
  • l'assistenza tecnica finalizzata a supportare dall'interno i processi di innovazione della PA regionale e la definizione di interventi finalizzati ad agevolare l'adozione e l'impatto delle ICT e di modelli operativi/gestionali innovativi nell'amministrazione pubblica;
  • l'assistenza tecnica alla PA regionale nella definizione, attuazione, monitoraggio, verifica e controllo degli interventi previsti dalla programmazione strategica regionale a sostegno dell'innovazione.

- la Società in house Puglia Sviluppo in base allo Statuto svolge i seguenti compiti: Svolgimento di attività riconducibili alla gestione di servizi di interesse generale svolti per conto della Regione Puglia e in particolare:

  • la realizzazione di attività di interesse generale in favore della Regione Puglia;
  • la promozione, nel territorio della Regione Puglia, della nascita di nuove imprese e dello sviluppo delle imprese esistenti;

• lo sviluppo della domanda di innovazione e dei sistemi locali di impresa, anche nei settori agricolo, turistico e del commercio;
• la progettualità dello sviluppo.

- Entrambe le Società hanno l'esperienza, la capacità e l'affidabilità in materia di protezione dei dati personali necessarie affinchè possa loro essere affidato l'incarico di Responsabile esterno e presentano idonee garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate a dimostrare il rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo della sicurezza.

Tenuto conto

- del modello organizzativo c.d. MAIA adottato dall'Amministrazione regionale, il quale coinvolge anche le Società in house (InnovaPuglia e Puglia Sviluppo), chiamate spesso a svolgere compiti e funzioni istituzionali per conto della Regione Puglia, sia sulla base di quanto previsto dai rispettivi Statuti sia sulla base di specifiche convenzioni o altri atti di affidamento adottati dai dirigenti o dai Direttori di Dipartimento regionali nell'esercizio delle funzioni ad essi affidati, si rende necessario per esigenze di omogeneità fornire a costoro delle indicazioni sui compiti generali e specifici da affidare alle Società in house quali Responsabili esterni del trattamento dei dati personali.
- I compiti dei Responsabili esterni del trattamento e le misure tecniche ed organizzative adeguate per garantire e dimostrare che il trattamento è conforme alla normativa sono indicati nell'Allegato A.
- Per ogni singolo affidamento alle due Società il Responsabile del trattamento interno (Dirigente di Sezione o Direttore di Dipartimento) referente per le attività assegnate alla Società in-house deve eseguire un pre-accertamento (pre-assessment) di impatto sulla protezione dei dati, avente ad oggetto i rischi afferenti al trattamento di dati personali riguardante le specifiche attività da svolgere, le misure tecniche ed organizzative, previste nell'allegato A, saranno implementate o specificate a seconda della tipologia e delle modalità di trattamento da eseguire per svolgere l'affidamento, utilizzando come schema di riferimento l'Allegato B.
- In seguito a quanto emerso dallo svolgimento di un pre-accertamento (pre-assessment) il referente per le attività assegnate alla Società in-house provvede se necessario ad eseguire una valutazione d'impatto sulla protezione dei dati eseguita (art. 35 Regolamento UE 2016/679).
- Tale analisi deve riguardare la natura e la finalità del trattamento, la tipologia dei dati (personali, giudiziali, sensibili, identificativi), la modalità del trattamento (automatizzato o meno) e la natura giuridica dell'interessato (dati di persone fisiche o giuridiche).

Si propone pertanto di designare come Responsabili esterni del trattamento dei dati personali le Società in house InnovaPuglia S.p.A. e Puglia Sviluppo S.p.A., nella persona dei legali rappresentanti delle Società, per lo svolgimento delle funzioni e dei compiti, svolti per conto della Regione Puglia, come definiti nei propri statuti, di approvare gli allegati A) e B) in cui si forniscono ai Responsabili interni del trattamento dati come individuati in base alla DGR. n. 2063/2016 le indicazioni sui compiti generali e su quelli specifici dei Responsabili esterni del trattamento dati, di disporre che i compiti specifici siano di volta in volta integrati ed individuati sulla base delle singole convenzioni o comunque degli atti di affidamento disposti dalle strutture regionali.

COPERTURA FINANZIARIA DI CUI AL D. LGS N.118/2011 E S. M. I.

La presente deliberazione non comporta implicazioni di natura finanziaria sia di entrata che di spesa e dalla stessa non deriva alcun onere a carico del bilancio regionale.

Il presente provvedimento è di competenza della Giunta regionale ai sensi dell'art. 44, comma 1, della L.R. n. 7/2004 "Statuto della Regione Puglia";

Il relatore, sulla base delle risultanze istruttorie come innanzi illustrate, propone alla Giunta l'adozione del conseguente atto finale,

LA GIUNTA REGIONALE

- Udita la relazione e la conseguente proposta del Presidente;
- Viste le sottoscrizioni poste in calce al presente provvedimento dal Dirigente della Sezione affari istituzionali e giuridici e dal segretario Generale della Presidenza G.r.;
- A voti unanimi espressi nei modi di legge;

DELIBERA:

- di prendere atto di quanto riportato in narrativa che qui si intende integralmente riportato;
- di designare, per le ragioni espresse in premessa, quali Responsabili "esterni" del Trattamento ai sensi dell'art. 29 del D.Lgs. 196/2003, per i trattamenti di dati personali, le proprie società in house InnovaPuglia S.p.A. e Puglia Sviluppo S.p.A. per lo svolgimento delle funzioni e compiti, svolti per conto della Regione Puglia, come definiti nei propri statuti;
- di approvare l'allegato A) quale parte integrante della presente deliberazione recante "Compiti del Responsabile esterno del trattamento di dati";
- di approvare l'allegato B) quale parte integrante della presente deliberazione recante "Schema sui compiti specifici del Responsabile esterni del Trattamento dei dati";
- di disporre per ogni singolo affidamento alle due Società di eseguire un pre-accertamento (pre-assessment) di impatto sulla protezione dei dati con una successiva ed eventuale esecuzione di una valutazione d'impatto sulla protezione dei dati eseguita (art. 35 Regolamento UE 2016/679), avente ad oggetto i rischi afferenti al trattamento di dati personali riguardante le specifiche attività da svolgere, le misure tecniche ed organizzative, previste nell'allegato A, saranno implementate o specificate a seconda della tipologia e delle modalità di trattamento da eseguire per svolgere l'affidamento.
- di disporre che, a corredo degli specifici affidamenti di cui al punto precedente, il Dirigente e/o il Direttore del Dipartimento della Regione responsabile di attività previste negli affidamenti comunichi alla Società quale Responsabile esterno del trattamento dei dati i compiti specifici, utilizzando lo schema di cui all'allegato B, e ne ottenga la copia controfirmata per accettazione dalla Società;
- di disporre la notificazione a cura della Segreteria generale della Presidenza g.r. del presente provvedimento a InnovaPuglia S.p.A., a Puglia Sviluppo S.p.A., nonché ai Direttori di Dipartimento e ai Dirigenti di Sezione per tutti gli oneri e adempimenti di competenza;
- di disporre la pubblicazione del presente provvedimento nel Bollettino Ufficiale e sul sito della Regione Puglia.

IL SEGRETARIO DELLA GIUNTA	**IL PRESIDENTE DELLA GIUNTA**
_____	_____

Il sottoscrittore attesta che il procedimento istruttorio ad esso affidato è stato espletato nel rispetto della vigente normativa regionale, nazionale e comunitaria e che il presente schema di provvedimento, dallo stesso predisposto ai fini dell'adozione dell'atto finale da parte della Giunta Regionale, è conforme alle risultanze istruttorie.

Il Dirigente della Sezione Affari Istituzionali e Giuridici

_____

Avv. Silvia Piemonte

Il Segretario Generale del Presidente

_____

Dott. Roberto Venneri

Presidente della Giunta Regionale

_____

Dott. Michele Emiliano

REGIONE PUGLIA

Allegato B

Schema sui compiti specifici del Responsabile esterno del Trattamento

1. Premessa

La Sezione di Dipartimento _____ della Regione Puglia, in qualità di Responsabile del trattamento dato in base alla DGR n. 2063 del 2016 e Referente per le attività assegnate alla Società in-house_____ nell'ambito dell'affidamento di cui al seguente Atto _____, in conformità a quanto previsto dalla DGR n. _____, con il presente atto assegna alla Società i seguenti compiti che prevedono il trattamento di dati personali.
In seguito allo svolgimento di un pre-accertamento (pre-assessment) di impatto sulla protezione dei dati, avente ad oggetto i rischi afferenti al trattamento di dati personali riguardante le specifiche attività da svolgere, le misure tecniche ed organizzative, **previste dall'Allegato A (di cui alla DGR. n. ……**, costituente parte integrante della presente convenzione, si indicano le implementazioni o specificazioni nelle modalità di trattamento da eseguire per svolgere l'affidamento.

- Natura e la finalità del trattamento

_____
_____
_____

- Tipologia dei dati (personali, giudiziali, sensibili, identificativi)

_____
_____
_____

- Modalità del trattamento (automatizzato o meno)

_____
_____
_____

- Natura giuridica dell'interessato (dati di persone fisiche o giuridiche)

_____
_____
_____

2. Con riguardo ai dati personali precedentemente descritti la Società deve:

- ☐ gestire in toto o in parte il procedimento amministrativo al servizio dell'utente
- ☐ gestire un'applicazione informatica e/o un sistema informatico che li contengono
- ☐ gestire l'assistenza all'utente in relazione alle procedure informatiche
- ☐ elaborare i dati per fornire informazioni di dettaglio e/o aggregate
- ☐ nominare gli incaricati del trattamento
- ☐ nominare gli Amministratori di Sistema
- ☐ incaricare come soggetto esterno del trattamento
- ☐ incaricare come soggetto esterno del trattamento una pubblica amministrazione o qualsiasi altro ente
- ☐ _____
- ☐ _____

- Sistema di Gestione della sicurezza delle informazioni (Certificazione ISO27001)

□ Il trattamento rientra nel Sistema di Gestione
□ Il trattamento rientra solo per le attività di gestione di un'applicazione informatica e/o di un sistema informatico
□ Il trattamento non rientra nel Sistema di Gestione

- Il trattamento dei dati presenta un rischio elevato in quanto rientra tra le seguenti fattispecie:

□ valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
□ trattamento, su larga scala, di categorie particolari di dati personali:
  □ l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
  □ relativi a condanne penali e a reati o a connesse misure di sicurezza

□ sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

□ _____

In seguito a quanto emerso dallo svolgimento di un pre-accertamento (pre-assessment) di impatto sulla protezione dei dati **non si ritiene** necessario provvedere ad eseguire una valutazione d'impatto sulla protezione dei dati eseguita (art. 35 Regolamento (UE) 2016/679).

In alternativa

In seguito a quanto emerso dallo svolgimento di un pre-accertamento (pre-assessment) di impatto sulla protezione dei dati **si ritiene** necessario provvedere ad eseguire una valutazione d'impatto sulla protezione dei dati eseguita seguendo quanto disposto dall'art. 35 Regolamento (UE) 2016/679 e quanto definito dalla Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" WP248 adottate dal Gruppo di lavoro Art. 29 il 4 aprile 2017:

Trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento
_____
_____
_____
Valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità
_____
_____
_____

Valutazione dei rischi per i diritti e le libertà degli interessati

_____
_____
_____

Misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

_____
_____
_____

Il Dirigente della

Sezione _____

Referente delle attività

(_____ _____)

Data _____

Per accettazione e per ricezione della documentazione

IL Legale Rappresentante della Società

(_____ _____)

Data _____

REGIONE PUGLIA

Allegato A

Compiti del Responsabile esterno del Trattamento dei dati

1. Premessa

I compiti dei Responsabili esterni del trattamento e le misure tecniche ed organizzative adeguate per garantire e dimostrare che il trattamento è conforme alla normativa sono indicati nel presente Allegato A.
Per ogni singolo affidamento alle due Società il Responsabile del trattamento interno (Dirigente di Sezione o Direttore di Dipartimento) referente per le attività assegnate alla Società in-house deve eseguire un pre-accertamento (pre-assessment) di impatto sulla protezione dei dati, avente ad oggetto i rischi afferenti al trattamento di dati personali riguardante le specifiche attività da svolgere, le misure tecniche ed organizzative, previste nel presente documento, saranno implementate o specificate a seconda della tipologia e delle modalità di trattamento da eseguire per svolgere l'affidamento, utilizzando l'Allegato B.
Tale accertamento deve riguardare la natura e la finalità del trattamento, la tipologia dei dati (personali, giudiziali, sensibili, identificativi), la modalità del trattamento (automatizzato o meno) e la natura giuridica dell'interessato (dati di persone fisiche o giuridiche).
In seguito a quanto emerso dallo svolgimento di un pre-accertamento (pre-assessment) il referente per le attività assegnate alla Società in-house provvede se necessario ad eseguire una valutazione d'impatto sulla protezione dei dati eseguita (art. 35 Regolamento UE 2016/679).

Si evidenzia che l'art. 29 comma 3 del D.Lgs. n. 196/2003 e s.m.i., prevede che "*Ove necessario per esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione di compiti*", per cui è possibile che le due Società vengano incaricate solo per alcuni compiti specifici, come ad esempio la sola gestione dei sistemi informatici preposti allo svolgimento di un procedimento. In casi come questo, gli adempimenti in generale ascrivibili ad un Responsabile del Trattamento come per esempio la garanzia del diritto all'oblio o l'esercizio dei diritti di cui all'art. 7, saranno di pertinenza del Responsabile interno del trattamento che gestisce il procedimento nella sua interezza, per quanto concerne la decisione circa l'applicabilità e portata degli interventi necessari, e del Responsabile esterno della gestione dei sistemi informatici per la sola effettiva attuazione degli interventi disposti dall'altro Responsabile

Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento (che può esprimersi anche attraverso i propri responsabili interni del trattamento). Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche.
Le Società in house della Regione Puglia possono trattare i dati personali "*comuni*" solo per svolgere le rispettive funzioni e i compiti previsti nei relativi Statuti.
Norme più stringenti, di seguito esaminate, disciplinano la comunicazione e la diffusione dei "dati comuni" (*art. 19, comma 2 e 3 del D.Lgs. 196/2003)*

Ai sensi dell'art. 4 del D.Lgs. 196/2003 si intende per:
a) "*trattamento*", qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione

e la distruzione di dati, anche se non registrati in una banca di dati;

b) "dato personale", qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;
c) "dati sensibili", i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni ed organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;
d) "dati giudiziari", i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.
e) “dati comuni”, i dati personali che, per esclusione, non appartengono alle predette categorie dei dati sensibili o giudiziari.

Ai sensi dell’art. 4 del Regolamento (UE) 2016/679 si intende per:

a) “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;
b) “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;
c) “limitazione di trattamento”: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro
d) “dati genetici”: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
e) “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;
f) “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;

Il trattamento dei dati sensibili o giudiziari, nondimeno, è consentito solo se è autorizzato da un’espressa disposizione di legge o di regolamento (nazionali o regionali) che specifichi i tipi di dati che possono essere trattati, le operazioni eseguibili sui dati medesimi e le finalità di rilevante interesse pubblico perseguite *(artt. 20 e 21 del D.Lgs. 196/2003)*.

Quando il trattamento è direttamente disciplinato dalla normativa di settore, devono essere scrupolosamente osservati presupposti, limiti e modalità di trattamento, rinvenibili direttamente o

desumibili dalla stessa, che rilevino ai fini del trattamento dei dati personali *(art. 18, comma 3, del D.Lgs. 196/2003)*.

Il Responsabile del trattamento deve garantire, attraverso misure tecniche e organizzative adeguate, la qualità dei dati, le corrette modalità di raccolta, conservazione e trattamento degli stessi, anche da parte del personale della propria struttura, in modo tale che il trattamento soddisfi i requisiti previsti dal Regolamento Europeo sul trattamento dei dati, Codice Privacy, dai Provvedimenti del Garante e dal presente documento e vigilare sul rispetto delle istruzioni impartite.

Le Società in house devono astenersi dal richiedere il consenso o un'autorizzazione al trattamento dei dati personali da parte degli interessati laddove svolgano attività istituzionale per conto dell'Amministrazione regionale (art. 18, comma 4, del D.Lgs. 196/2003)[1].
In tutti gli altri casi, il consenso è richiesto, atteso che le Società sono soggetti privati, nonché quando operano in ambito sanitario (artt. 18, comma 4, 23, 76 e ss. del D.Lgs. 196/2003).

Ai sensi dell'art. 9 del Regolamento (UE) 2016/679 non occorre il consenso dell'interessato nel caso in cui il trattamento è necessario: per motivi di interesse pubblico; per la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici; a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici.

2. Organizzazione.

Il Responsabile esterno del trattamento può nominare, per iscritto, i propri collaboratori, interni ed esterni, incaricati del trattamento (*art. 30 del D.Lgs. 196/2003*) o comunque autorizzati al trattamento, individuando l'ambito del trattamento consentito ad ognuno, in base alle mansioni svolte, e impartendo istruzioni scritte per garantire che ciascun collaboratore tratti dati personali strettamente indispensabili per lo svolgimento dell'attività svolta, nel pieno rispetto del Codice Privacy, delle presenti istruzioni e di quanto egli stesso ritenga necessario in base alla tipologia dei trattamenti dei dati effettuati dalla propria struttura. E' ammissibile anche la documentata preposizione attraverso l'unità organizzativa e/o operativa di appartenenza.

Se al soggetto esterno è affidata l'amministrazione di sistemi informatici, esso deve essere investito dal Responsabile (interno) anche del compito di nominare gli Amministratori di Sistema, ai sensi del Provvedimento del Garante del 27.11.2008 sugli Amministratori di Sistema.
L' "Amministratore di Sistema": è, in ambito informatico, la figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi quali i sistemi ERP (Enterprise resource planning), le reti locali e gli apparati di sicurezza, nella misura in cui tali attività di gestione e manutenzione consentano di intervenire sui dati personali.

3. Informativa.

Gli Interessati devono ricevere un'idonea e preventiva Informativa concisa, trasparente, intelligibile per l'interessato e facilmente accessibile, circa modalità le modalità del trattamento dei loro dati

[1] Una parziale deroga alla regola predetta è, nondimeno, accettata in materia di immagini e filmati per i quali si preveda la diffusione, in particolare nel caso di dati personali di minori.

personali *(art. 13 del D.Lgs. 196/2003 e artt. 13 e 14 del* Regolamento (UE) 2016/679*)*. Tale adempimento deve essere svolto nel momento in cui i dati personali sono ottenuti, nel caso in cui i dati personali non siano stati ottenuti presso l'interessato, entro un termine ragionevole che non può superare 1 mese dalla raccolta, oppure al momento della prima comunicazione all'interessato (con compilazione di moduli o *format on line*, etc.).

L'interessato, o la persona presso la quale sono raccolti i dati personali, sono previamente informati per iscritto circa:

a) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
b) la natura obbligatoria (in base a quale norma di legge o contrattuale) o facoltativa del conferimento dei dati, se riguarda un requisito necessario per la conclusione di un contratto, indicando le possibili conseguenze della mancata comunicazione di tali dati;
c) i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito eventuale di diffusione dei dati medesimi (indicando altresì la norma di legge che autorizza la diffusione);
d) le categorie di dati personali e la fonte da cui hanno origine e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico;
e) i diritti di chiedere al titolare del trattamento (o al Responsabile interno o esterno, a seconda di chi detenga e tratti il dato) l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento dei dati personali che lo riguardano e di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
f) gli estremi identificativi del Titolare, del Responsabile (interno ed esterno) del trattamento e del Responsabile della protezione dei dati (Data Protection Officer), indicando il recapito a cui l'interessato può rivolgersi per l'esercizio dei diritti e di presentare un reclamo all'autorità di controllo;
g) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
h) l'eventuale trasferimento i dati personali in Paesi terzi e, in caso affermativo, attraverso quali strumenti periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione;
i) il diritto di presentare un reclamo all'autorità di controllo
j) l'esistenza di un processo decisionale automatizzato, compresa la profilazione e in tali casi la logica utilizzata;
k) i legittimi interessi perseguiti dal titolare del trattamento o da terzi nel caso siano necessari per il trattamento.

5. Comunicazione e diffusione dei dati. Pubblicazione di atti.

La comunicazione di dati personali da parte della Società in house a pubbliche Amministrazioni (*effettuata in qualunque forma*, *anche previa convenzione*, *ed in assenza di nomina del Responsabile "esterno"*) è ammessa quando 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, ovvero prevista da una norma di legge o di regolamento (art. 6 del Regolamento (UE) 2016/679).

In mancanza di tale norma la comunicazione è ammessa quando è comunque necessaria per lo svolgimento di funzioni istituzionali e può essere iniziata se è stata data previa informazione (tramite PEC a urp@pec.gpdp.it) al Garante Privacy delle circostanze e motivazioni per cui si intende effettuare la comunicazione ad altra Pubblica Amministrazione ed il Garante Privacy non si è espresso in senso contrario entro 45 giorni dal ricevimento della predetta comunicazione (*art. 19, comma 2, del D.Lgs. 196/2003).*

Ai sensi del D.Lgs. 196/2003 si distinguono:

1) "comunicazione", il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

   Lo scambio di dati tra strutture afferenti alla stessa Società o tra questa le strutture amministrative della Giunta Regionale non costituisce comunicazione.

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

   La principale forma di “diffusione” è data dalla pubblicazione di dati personali, direttamente o contenuti in atti e documenti, nel sito web della Società o dell’Amministrazione regionale e nei siti tematici dell’Amministrazione regionale.

Per quanto riguarda la pubblicazione di atti e documenti contenenti dati personali e/o la divulgazione di dati personali attraverso i siti internet della società in house, poiché queste azioni determinano una "diffusione" di dati personali, comportando la conoscenza dei dati da parte di un numero indeterminato di cittadini, devono essere adottate opportune cautele riguardo i dati personali pubblicati.
E’ quindi fondamentale che fin dalla stesura dei provvedimenti destinati alla pubblicazione, si valuti con estrema attenzione la necessità o meno di inserire dati personali e la tipologia degli stessi.

Sul tema si possono consultare le Linee Guida (2011) del Garante Privacy in materia di trattamento di dati personali, effettuato da soggetti pubblici per finalità di pubblicazione e di diffusione sul web di atti e documenti. Tali Linee Guida forniscono utili esemplificazioni.

Non devono essere in alcun caso diffuse *on line* o riportate negli atti pubblicati nel *web*, informazioni idonee a rivelare lo stato di salute degli interessati (*artt. 22, comma 8, e 68, comma 3, del D.Lgs. 196/2003*).

Si pensi, in tale ultimo caso, all'indicazione:
- dei titoli dell'erogazione dei benefici (es. attribuzione di borse di studio a "*soggetto portatore di handicap*", o riconoscimento di buono sociale a favore di "*anziano non autosufficiente*" o con l'indicazione, insieme al dato anagrafico, delle specifiche patologie sofferte dal beneficiario);
- dei criteri di attribuzione (es. punteggi attribuiti con l'indicazione degli "*indici di autosufficienza nelle attività della vita quotidiana*");
- della destinazione dei contributi erogati (es. contributo per "*ricovero in struttura sanitaria oncologica*").

6. Diritto d’accesso e altri diritti dell’interessato

Gli Interessati hanno diritto di accedere ai propri dati *(art 12 paragrafo 3 del* Regolamento (UE) 2016/679 e art. 7 e ss del D.Lgs. 196/2003*)*.
Il Responsabile esterno deve fornire il riscontro all'Interessato entro 1 mese, estendibile fino a 3 mesi in casi di particolare complessità. L'interessato può presentare istanza di riesame al Titolare del trattamento, il quale si pronuncia entro 30 gg.

In base all'art. 7, D.lgs. 196/2003
1. L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.
2. L'interessato ha diritto di ottenere l'indicazione:
a) dell'origine dei dati personali;
b) delle finalità e modalità del trattamento;
c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2;
e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.
3. L'interessato ha diritto di ottenere:
a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;
b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.
4. L'interessato ha diritto di opporsi, in tutto o in parte:
a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;
b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

Il responsabile fornirà gratuitamente le informazioni relative al trattamento dei dati.
In caso di richieste manifestamente infondate o eccessive, in particolare per il loro carattere ripetitivo, il Responsabile ne da comunicazione al Titolare del trattamento (o, per esso, al Responsabile interno eventualmente individuato).
Nel caso di istanze particolarmente complesse il Responsabile può richiedere un confronto con il Titolare del trattamento (o, per esso, al Responsabile interno eventualmente individuato), affinchè valutino unitamente la complessità del riscontro all'interessato e per stabilire l'ammontare dell'eventuale contributo da chiedere all'interessato in ragione dei costi amministrativi da sostenere.
Il responsabile da riscontro all'interessato, preferibilmente mediante l'invio di una email all'indirizzo indicato dall'interessato.

7. Sicurezza informatica

I dati personali, siano essi trattati in formato digitale oppure in formato cartaceo, devono essere custoditi con cura al fine di preservarne le caratteristiche di integrità, disponibilità e confidenzialità. Il responsabile del trattamento deve adottare idonee misure tecniche e organizzative per garantire la sicurezza dei trattamenti (ex art. 32 Regolamento (UE) 2016/679)

L'adozione delle misure tecniche e organizzative devono tener conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.

Le misure tecniche ed organizzative saranno riportate nell'allegato B, in seguito alla valutazione preventiva di impatto sulla protezione dei dati effettuata per ogni singolo servizio affidato alla società in house.

Tale valutazione deve tener conto dei rischi derivanti dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

In ragione del fatto che i trattamenti possono essere effettuati con o senza l'ausilio di strumenti elettronici, le misure di sicurezza da adottare devono essere differenti ed adeguate alle diverse situazioni ed alla natura dei dati trattati, come più ampiamente descritto di seguito.

Rientra, in ogni caso, nei compiti del Responsabile l'adozione di ulteriori e più adeguate misure di sicurezza, ritenute necessarie per la particolare tipologia dei dati trattati e della modalità del trattamento.

Il responsabile del trattamento in accordo con il referente regionale (ossia il Responsabile interno o direttamente con il titolare) valuterà l'applicazione delle seguenti misure:

a) misure di protezione dei dati personali quali ad esempio la pseudonimizzazione e/o la cifratura;

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

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

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

a) il trattamento di dati personali con strumenti elettronici è consentito solo agli "Incaricati", dotati di credenziali di autenticazione univoche. Il Responsabile deve istruire gli Incaricati sulla necessaria cautela da adottare per assicurare la segretezza e la custodia delle credenziali. Le predette credenziali di autenticazione non possono essere assegnate ad altri Incaricati, neppure in tempi diversi. (Art. 34, comma 1, lett. a) del D.Lgs. 196/2003).

Le credenziali di autenticazione più diffuse sono la coppia: "nome utente" e "password".

b) nel caso di mancato utilizzo delle credenziali per un periodo superiore a tre mesi e/o di perdita, da parte di un Incaricato, della qualità che consente l'accesso ai dati, il Responsabile deve richiedere la disattivazione delle credenziali del predetto Incaricato. Tale regola opera esclusivamente per le credenziali di autenticazione per le applicazioni in uso alle singole strutture e non per le credenziali di attestazione al dominio.

L'attestazione al dominio si ha all'avvio del sistema con la digitazione delle credenziali di autenticazione e consente di fruire delle funzionalità disponibili in dominio (Internet, posta elettronica, ecc.).

Il Responsabile deve individuare modalità organizzative per consentire, in caso di prolungata assenza o impedimento dell'Incaricato, qualora lo stesso sia l'unico incaricato con quelle specifiche autorizzazioni di accesso, la disponibilità dei dati e degli strumenti elettronici ad esso assegnati, mediante la nomina (per iscritto) di un "*custode delle password*" a livello di struttura ovvero promuovendo l'individuazione, direttamente da parte del lavoratore interessato dall'assenza, di un "*delegato fiduciario*" che acceda a tutte le risorse necessarie in sua assenza. *(Art. 34, comma 1, lett. b) del D.Lgs. 196/2003)*.
Il "*custode delle password*" e/o il "*delegato fiduciario*" sono figure particolarmente funzionali laddove le credenziali di autenticazione, diverse da quelle di dominio, riguardino l'accesso a "Banche dati" o ad applicativi per lo svolgimento delle funzioni istituzionali e la cui mancata fruizione, dovuta all'assenza dell'Incaricato, comporti un rallentamento non ammissibile per l'attività amministrativa.
L'accesso, resosi necessario in caso di assenza dell'Incaricato impone al Responsabile di informare tempestivamente lo stesso Incaricato dell'intervento effettuato, avvalendosi delle credenziali depositate presso il "*custode delle password*" o presso il "*delegato fiduciario*".

c) Il Responsabile, prima dell'inizio del trattamento con l'utilizzo di applicativi, individua l'ambito del trattamento consentito ai singoli Incaricati e richiede per l'incaricato l'attribuzione del "profilo di autorizzazione" adeguato all'ambito di trattamento consentito al medesimo.
Il Responsabile deve inoltre verificare periodicamente, con cadenza almeno annuale, la sussistenza delle condizioni per la conservazione del profilo di autorizzazione assegnato all'Incaricato. Il Responsabile, definite o modificate le facoltà operative attribuite allo stesso, deve dare comunicazione tempestiva per l'adeguamento del profilo (privilegi di accesso). (Art. 34, comma 1, lett. c) e lett. d) del D.Lgs. 196/2003)

I "profili di autorizzazione" sono l'insieme delle facoltà operative/operazioni, tecnicamente consentite dal sistema informatico/applicativo all'Incaricato, in relazione all'ambito di trattamento consentito al medesimo.

d) con riguardo alla protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici, il Responsabile deve vietare all'Incaricato di comunicare ad altri le proprie credenziali nonché di usare le credenziali di altri Incaricati, salvo quanto disposto alla precedente lett. b).
Il Responsabile deve garantire la costante attivazione del software antivirus dando disposizioni agli Incaricati di segnalare prontamente ogni eventuale malfunzionamento o anomalia di funzionamento della postazione di lavoro.
Il Responsabile deve, altresì, ricordare ai lavoratori che non è consentita:
1) l'installazione di qualsiasi *software* che non sia debitamente autorizzato (*potendo l'installazione di un software alterare – indipendentemente dalla volontà dell'utilizzatore – la funzionalità delle postazioni di lavoro, sia sotto il profilo dell'integrità, disponibilità e riservatezza dei dati sia del collegamento in rete*);
3) la creazione e l'utilizzazione di "cartelle condivise", che contengano dati personali, senza l'impostazione nominativa della condivisione e senza l'eliminazione della voce "*everyone*"

dalle “autorizzazioni condivisione” (*diversamente l’accesso alla cartella sarebbe incontrollato*).
(*Art. 34, comma 1, lett. e) del D.Lgs. 196/2003*).

e) limitatamente all’adozione di procedure per la custodia di copie di sicurezza ed il ripristino della disponibilità dei dati, il Responsabile deve dare disposizioni affinché gli Incaricati effettuino periodici backup dei dati non replicati in altre aree (ad es. dati che risiedono unicamente su una postazione di lavoro, c.d. “in locale”), con cadenza almeno settimanale se trattasi di dati sensibili e giudiziari. Eventuali copie-immagine atte al ripristino del sistema devono essere custodite accuratamente.
(Art. 34, comma 1, lett. f) del D.Lgs. 196/2003).

f) Nel caso di dati personali sensibili e giudiziari memorizzati “localmente” sulle stazioni di lavoro (desktop, PC portatili, palmari, etc.) situate presso la propria struttura, il Responsabile ha facoltà, a propria discrezione, di adottare - con proprio decreto - un “Documento sulla Sicurezza” che descriva le misure minime indicate all’art. 34 D.Lgs. 196/2003[2].

g) per determinati trattamenti, relativi a dati idonei a rivelare lo stato di salute o la vita sessuale (ad es. banche dati sanitarie), è necessario adottare tecniche di cifratura dei dati o codificazione degli interessati o delle informazioni.
Il Responsabile, nel caso di specie, deve assicurarsi che i software utilizzati siano dotati di cifratura e di autenticazione forte (ad es. smart card).
(Art. 34, comma 1, lett. h) del D.Lgs. 196/2003).

8. Ulteriori compiti dei Responsabili

Costituiscono ulteriori compiti del Responsabile:

1) disporre l’adozione dei provvedimenti imposti dal Garante quale misura conseguente all’accoglimento delle richieste degli interessati, dandone comunicazione al Dirigente o al Direttore di Dipartimento regionali competenti per materia in base alla DGR. n. 2063 del 21.12.2016;
2) predisporre la documentazione e gli atti necessari per il Garante nei casi e nei modi previsti dalla normativa, dandone comunicazione al Dirigente o al Direttore di Dipartimento regionali competenti per materia in base alla DGR. n. 2063 del 21.12.2016.
3) Valutare la necessità di nominare, con propri atti, Incaricati del trattamento, Amministratori di Sistema e Subresponsabili, in quest’ultimo caso previa autorizzazione preventiva del Titolare.
4) Nominare entro il 25 maggio 2018 il Responsabile della protezione dei dati (Data Protection Officer) in funzione delle qualità professionali, della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i propri compiti. Il nominativo sarà comunicato al Garante per la protezione dei dati.
5) Redigere il “Registro delle attività di trattamento” contente:
   a) Nome e dati di contatto del/i Responsabile/i, del Titolare per cui egli agisce, del rappresentante del Titolare o del Responsabile e del DPO;
   b) Categorie dei trattamenti effettuati per conto di ogni Titolare;
   c) ove applicabile, i trasferimenti di dati personali verso un Paese terzo o un’organizzazione internazionale identificati e eventuali garanzie;

[2] L’obbligo di cui all’ art. 34, comma 1, lett. g, del D.Lgs. 196/2003 della "*tenuta di un aggiornato documento programmatico sulla sicurezza*" è venuto meno con l'art. 45, comma 1, lett. c), del D.L. 9 febbraio 2012, n. 5, convertito, con modificazioni, dalla L. 4 aprile 2012, n. 35.

d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative adottate.

6) Garantire il rispetto del Diritto all'oblio dell'interessato ad ottenere, senza giustificato ritardo, la cancellazione dei propri dati personali che non siano più necessari per le finalità per le quali sono stati raccolti o altrimenti trattati, o quando l'interessato abbia revocato il proprio consenso, o si sia opposto al trattamento dei dati personali che lo riguardano, o quando il trattamento dei suoi dati personali non sia altrimenti conforme al Regolamento.
7) Agevolare con appositi strumenti informatici o procedure il diritto dell'interessato di trasmettere o ottenere la trasmissione di propri dati personali ad un altro Titolare, al fine di eliminare ogni impedimenti.
8) Segnalare eventuali variazioni del rischio rappresentato dalle attività relative al trattamento, al fine di valutare se riesaminare la valutazione d'impatto sulla protezione dei dati (ex art. 35 paragrafo 11 Regolamento (UE) 2016/679)

9. Notifica delle violazioni di dati personali

Il responsabile del trattamento deve comunicare al titolare del trattamento le violazioni di dati personali nel momento in cui viene a conoscenza, fornendo gli elementi necessari per valutare se da tale violazione derivino rischi per i diritti e le libertà degli interessati, al fine di adempiere quanto disposto dall'art. 33 del Regolamento (UE) 2016/679.
In particolare il responsabile del trattamento deve fornire:

a) natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
b) il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
c) conseguenze della violazione dei dati personali;
d) indicazioni sulle misure adottate per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.