OSSERVATORIO DI EPIDEMIOLOGIA
DECRETO DEL COORDINATORE

n. 12 del 03/06/2013

Oggetto: **Decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali) ss.mm. –. Nomina degli incaricati dei trattamenti di dati personali di competenza del Coordinatore Osservatorio di epidemiologia – Progetto "Sorveglianza della mortalità materna: progetto pilota in Regioni del Nord, Centro e Sud Italia"**

IL COORDINATORE

Vista la legge regionale 24 febbraio 2005, n. 40 (*Disciplina del servizio sanitario regionale*) e successive modificazioni ed integrazioni e, specificatamente, l'art. 82-duodecies della stessa, con cui si definiscono le strutture organizzative dell'ARS;

Visto il decreto del Direttore dell'ARS n. 22 del 30/11/2011 con il quale è stato deciso di affidare al sottoscritto in via straordinaria la responsabilità dell'Osservatorio di Epidemiologia per l'esercizio delle funzioni ad esso attribuite, per il periodo necessario alla nomina del nuovo Coordinatore;

Visto il decreto legislativo 30 giugno 2003, n. 196 "*Codice in materia di protezione dei dati personali"*, di seguito nominato "Codice"e relative disposizioni attuative del Garante;

Richiamato, in particolare, l'art. 29 del medesimo Codice che disciplina la figura del responsabile del trattamento dei dati, definendone compiti e responsabilità;

Considerato che la normativa citata sottopone le pubbliche amministrazioni ad uno speciale regime giuridico, finalizzato a assicurare la tutela della riservatezza e la protezione dei dati personali in relazione ai trattamenti che avvengono in ambito pubblico;

Preso atto della deliberazione della Giunta regionale n. 167 del 12/03/2007 *"Direttiva per l'attuazione del decreto legislativo n. 196/2003 recante "Codice in materia di protezione di dati personali"* ;

Visti, altresì:

a) la deliberazione del Consiglio di Amministrazione n. 18 del 28 giugno 2004 e successive modificazioni, con cui si è proceduto ad nominare, in attuazione degli articoli 28 e 29 del richiamato Codice, i quali Responsabili del trattamento dati personali il coordinatore dell'osservatorio di epidemiologia per i trattamenti afferenti all'osservatorio di competenza e il coordinatore dell'osservatorio per la qualità e l'equità per i trattamenti afferenti all'osservatorio di competenza, impartendo loro specifiche istruzioni, ivi compreso il profilo di sicurezza; tra queste è previsto l'obbligo di procedere alla nomina degli incaricati del trattamento dei dati personali assegnati alla propria struttura;

b) il decreto del direttore n. 14 del 25 ottobre 2011, con il quale, tra l'altro, si è preso atto che il responsabile del trattamento dei dati afferenti all'Osservatorio di epidemiologia è il coordinatore dell'Osservatorio medesimo;

Considerato che a partire dal 20/03/2012 fino al 18/03/2014 è stato attivato un progetto denominato "Sorveglianza della mortalità materna: progetto pilota in Regioni del Nord, Centro e Sud Italia", avente ad oggetto l'attivazione di un sistema di sorveglianza della mortalità materna in Toscana, coordinato dall'Istituto Superiore di Sanità;

Visto che per lo svolgimento dell'attività relativa al progetto, le professionalità sotto indicate dovranno accedere ad alcuni flussi, nello specifico: modulistica relativa le morti materne avvenute in Toscana e relative copie di cartelle cliniche anonimizzate al fine di validare la causa di morte e valutare la qualità del processo assistenziale;

Ritenuto opportuno procedere, ai sensi dell'art. 30 del più volte citato Codice, alla nomina nell'ambito dell'attività di cui ai paragrafi che precedono:

- Antonella Cinotti nato a Firenze il 25/07/1956 dell'Università di Firenze incaricato esterno;
- Mariarosaria Di Tommaso nato a Melfi (PZ) il 22/06/1955, dell'Università di Firenze incaricato esterno;
- Valeria Dubini nato a Firenze il 08/10/1955 dell'Azienda USL 10 di Firenze incaricato esterno;
- Luigi Gagliardi nato a Milano il 07/09/1956, dell'Azienda USL 12 di Viareggio incaricato esterno;
- Carlo Giolli nato a Lucca il 17/05/1959, dell'Azienda USL 10 di Firenze incaricato esterno;
- Vincenzo Nardini nato a Napoli il 21/12/1963, dell'Azienda Ospedaliero-Universitaria Pisana incaricato esterno;
- Armando Pedullà nato a Catanzaro il 11/07/1952, dell'Azienda USL 10 di Firenze incaricato esterno;
- Riccardo Tartaglia nato a Napoli il 20/06/1954 dell'Azienda Regione Toscana incaricato esterno;
- Francesco Venneri nato a Cosenza il 25/06/1956 dell'Azienda USL 10 di Firenze incaricato esterno;
- Fabio Voller Dipendente ARS Dirigente Settore Osservatorio di Epidemiologia incaricato interno;
- Monica Da Frè Dipendente ARS Categoria D incaricato interno,

identificati nell'elenco allegato sub. lett. "A", parte integrante e sostanziale del presente provvedimento, in cui sono individuati i profili di autorizzazione e, quindi, le operazioni eseguibili, nonché l'ambito del trattamento consentito (per le operazioni svolte da ciascun incaricato per propria competenza), fornendo le specifiche istruzioni di cui all'Allegato sub. lett. "B", parte integrante e sostanziale del presente atto, che recepiscono i contenuti essenziali della richiamata direttiva regionale, adeguandoli alle esigenze organizzative dell'Ente;

Ritenuto altresì di precisare che nel richiamato allegato sub. lett. A i nominativi degli incaricati contrassegnati con un asterisco sono nominati d'intesa tra il responsabile del trattamento dati del settore amministrazione e il responsabile dell'osservatorio indicato; gli incaricati contrassegnati con doppio asterisco sono nominati d'intesa tra i due responsabili delle strutture organizzative di ARS;

DECRETA

1. di nominare, ai sensi dell'art. 30 del più volte citato Codice, nell'ambito del progetto: "Sorveglianza della mortalità materna: progetto pilota in Regioni del Nord, Centro e Sud Italia", avente ad oggetto l'analisi della modulistica relativa le morti materne avvenute in Toscana e relative copie di cartelle cliniche anonimizzate al fine di validare la causa di morte e valutare la qualità del processo assistenziale:
   - Antonella Cinotti nato a Firenze il 25/07/1956 dell'Università di Firenze incaricato esterno;
   - Mariarosaria Di Tommaso nato a Melfi (PZ) il 22/06/1955, dell'Università di Firenze incaricato esterno;
   - Valeria Dubini nato a Firenze il 08/10/1955 dell'Azienda USL 10 di Firenze incaricato esterno;
   - Luigi Gagliardi nato a Milano il 07/09/1956, dell'Azienda USL 12 di Viareggio incaricato esterno;
   - Carlo Giolli nato a Lucca il 17/05/1959, dell'Azienda USL 10 di Firenze incaricato esterno;
   - Vincenzo Nardini nato a Napoli il 21/12/1963, dell'Azienda Ospedaliero-Universitaria Pisana incaricato esterno;
   - Armando Pedullà nato a Catanzaro il 11/07/1952, dell'Azienda USL 10 di Firenze incaricato esterno;
   - Riccardo Tartaglia nato a Napoli il 20/06/1954 dell'Azienda Regione Toscana incaricato esterno;
   - Francesco Venneri nato a Cosenza il 25/06/1956 dell'Azienda USL 10 di Firenze incaricato esterno;
   - Fabio Voller Dipendente ARS Dirigente Settore Osservatorio di Epidemiologia, incaricato interno;
   - Monica Da Frè Dipendente ARS Categoria D, incaricato interno,

   identificati nell'elenco allegato sub. lett. "A", parte integrante e sostanziale del presente provvedimento, in cui sono individuati i profili di autorizzazione e, quindi, le operazioni eseguibili, nonché l'ambito del trattamento consentito (per le operazioni svolte da ciascun incaricato per propria competenza);
2. di impartire le prescrizioni contenute nell'allegato sub. lett. "B", parte integrante del presente atto, che recepiscono i contenuti essenziali della richiamata direttiva regionale n. 167/2007, adeguandoli alle esigenze organizzative dell'Ente;
3. di stabilire che gli incaricati al trattamento, così come identificati al punto 1, devono attenersi scrupolosamente alle prescrizioni richiamate al punto 2.
4. di assicurare, ai sensi dell'art. 1 della legge 7 agosto 1990, n. 241 e ss.mm. e dell'art. 32 della legge n. 69/2009, la pubblicità integrale del presente provvedimento mediante inserimento nella sezione "*Trasparenza*" sul sito web dell'ARS (www.ars.toscana.it).

Il f.f. Coordinatore
dell'Osservatorio di Epidemiologia
(Dott. Fabio Voller)

Allegato "A"

ARS TOSCANA
agenzia regionale di sanità

AGENZIA REGIONALE DI SANITA'

TRATTAMENTO DATI PERSONALI

OSSERVATORIO DI EPIDEMIOLOGIA

ELENCO DEGLI INCARICATI NOMINATI PER IL TRATTAMENTO

SST Servizio Sanitario della Toscana

Elenco degli incaricati al trattamento **OE e OQ**

PREMESSA

Con riferimento all'art 17, par. 3, dir. 95/46/CE, art. 8, comma 5, e 19, l. 695/1996 e art. 30 del "Codice", con il presente documento si provvede ad elencare gli incaricati nominati per il trattamento dei dati sensibili afferenti **all'Osservatorio di epidemiologia e all'osservatorio per la qualità e l'equità** dell'Agenzia regionale di sanità.
Si procede, altresì, all'assegnazione dei profili e, quindi, delle operazioni autorizzate, come definititi con deliberazione del CdA n. 18 del 28/06/2004 e successive modificazioni, con relativa indicazione dell'ambito di trattamento consentito, (cfr. art. 30, co. 2 del "Codice")[1].
E', infine, individuato l'archivio cui afferiscono i dati *de quibus*, in stretta correlazione con il CE.TRA (Censimento del trattamento dei dati) istituito presso l'ARS.

id	archivio	descrizione	prof	nominativo
	Sorveglianza mortalità materna	schede cartacee casi di morte materna e copie di cartelle cliniche	Amministratore banca dati specifica	Fabio Voller
	Sorveglianza mortalità materna	schede cartacee casi di morte materna e copie di cartelle cliniche	Amministratore banca dati specifica	Monica Da Frè
	Sorveglianza mortalità materna	schede cartacee casi di morte materna e copie di cartelle cliniche	Amministratore banca dati specifica	Antonella Cinotti
	Sorveglianza mortalità materna	schede cartacee casi di morte materna e copie di cartelle cliniche	Amministratore banca dati specifica	Mariarosaria Di Tommaso
	Sorveglianza mortalità materna	schede cartacee casi di morte materna e copie di cartelle cliniche	Amministratore banca dati specifica	Valeria Dubini
	Sorveglianza mortalità materna	schede cartacee casi di morte materna e copie di cartelle cliniche	Amministratore banca dati specifica	Luigi Gagliardi
	Sorveglianza mortalità materna	schede cartacee casi di morte materna e copie di cartelle cliniche	Amministratore banca dati specifica	Carlo Giolli
	Sorveglianza mortalità materna	schede cartacee casi di morte materna e copie di cartelle cliniche	Amministratore banca dati specifica	Vincenzo Nardini
	Sorveglianza mortalità materna	schede cartacee casi di morte materna e copie di cartelle cliniche	Amministratore banca dati specifica	Armando Pedullà
	Sorveglianza mortalità materna	schede cartacee casi di morte materna e copie di cartelle cliniche	Amministratore banca dati specifica	Riccardo Tartaglia
	Sorveglianza mortalità materna	schede cartacee casi di morte materna e copie di cartelle cliniche	Amministratore banca dati specifica	Francesco Venneri

[1] *"si considera tale anche la documentata preposizione della persona fisica ad una unità per la quale è individuato per iscritto l'ambito del trattamento consentito agli addetti dell'unità medesima"*

Allegato "B"

AGENZIA REGIONALE DI SANITA'

TRATTAMENTO DATI PERSONALI
afferenti alle strutture organizzative di ARS:

OSSERVATORIO DI "EPIDEMIOLOGIA"

OSSERVATORIO "PER LA QUALITA'"

"DIREZIONE"

ISTRUZIONI IMPARTITE DAI RESPONSABILI DEL TRATTAMENTO AGLI INCARICATI

(ex art. 30 decreto legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali"

INDICE

PREMESSA

Con il presente documento si provvede ad impartire agli incaricati dell'Agenzia Regionale di Sanità nominati per il trattamento dei dati personali e, specificatamente, di quelli sensibili e giudiziari, precise istruzioni, cui i medesimi debbono attenersi, ivi compreso il profilo della sicurezza. (Cfr.: art 17, par. 3, dir. 95/46/CE; art. 8, comma 5 e 19 l. 695/1996; art. 30 del "Codice").

Il documento consolida il processo di regolazione della materia già avviato dall'Agenzia, con l'intento di permettere a tutti gli addetti di operare nel quadro di indicazioni certe, che non devono essere intese come ulteriore appesantimento burocratico, ma come miglioramento della qualità del servizio offerto ai cittadini.
Lo scopo che si persegue è anche quello di fornire un *vademecum* operativo per coloro che quotidianamente dovranno confrontarsi con gli adempimenti in materia di privacy.

La nuova legge italiana per la tutela della riservatezza (Decreto legislativo 30 giugno 2003, n. 196, pubblicato in G.U. 29 luglio 2003, Serie generale n. 174, Supplemento ordinario n. 123/L) è germinato in un ambiente culturalmente ostile e solo la sensibilità giuridica e culturale di chi deve vigilare sull'applicazione di tale strumento normativo potrà consentire che nel nostro paese maturi una forte consapevolezza in materia di privacy.
Il diritto alla privacy rientra nelle libertà fondamentali dell'individuo; trova riconoscimento nella Carta dei Diritti Fondamentali dell'Unione Europea in quanto diritto alla dignità della persona.

L'*animus*, che caratterizza il presente lavoro, prende le mosse proprio dall'ambizione di diffondere quella che può agevolmente essere definita una **cultura della riservatezza**, che esprime nel nostro ordinamento un atto di alta civiltà.
Si apre un percorso probabilmente complesso, che almeno inizialmente e sotto certi aspetti, si presenterà come tassativamente applicativo delle norme di legge, ma che ci auguriamo possa far scaturire in coloro che vi parteciperanno un profondo senso della privacy, radicato al punto di confluire nel loro bagaglio culturale quotidiano e nella propria *forma mentis*.
La trattazione, pertanto, prefiggendosi uno scopo così elevato non si limiterà ad elencare quelle azioni lecite e quelle vietate, ma si preoccuperà di spiegare le ragioni delle azioni richieste dal Codice, ritenendo tale metodologia più efficace per introdurre l'approccio corretto alle norme in materia, che non possono rimanere mere astrazioni.

Sotto tale egida, ARS si è mossa, fra i primi nel panorama regionale, attraverso l'adozione di atti, che tutelano il suo operato.
L'attività di ARS si è così articolata:

1. **Deliberazione CdA 28 giugno 2004, n. 18** "Decreto legislativo 30 giugno 2003, n. 196 *(Codice in materia di protezione dei dati personali) – Ex artt. 28 e 29 - Nomina dei Responsabili trattamento dati personali – Istruzioni* e successive modificazioni, atto adottato per l'affidamento dei compiti dal Titolare al Responsabile (comma 4) e definizione delle istruzioni, ivi compreso il profilo della sicurezza, (cfr. art 16, dir. 95/46/CE; art. 8, comma 1, l. 695/1996; art. 29 del

"Codice"), nonché per l'istituzione del Gruppo Privacy e del censimento del trattamento dei dati (CE.TRA).

2. **16/07/2004** Notificazione al Garante, mediante modello telematico con firma digitale dell'intermediario convenzionato (art. 37).
3. **Decreto del Segretario Amministrativo del 27 luglio 2004, n. 45** "*Decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali)-Gruppo privacy-Nomina componenti*";
4. **Determinazione n. 1 del Coord. Oss. Epidemiologia del 1/12/2004** "*Gestione Registro Regionale AIDS- Nomina incaricati del trattamento dei dati personali*". In occasione della necessità di gestire il registro AIDS, attraverso la determinazione del 1/12/2004, si è anticipata la nomina di alcuna incaricati, fornendo loro anche le istruzioni necessarie all'attività da svolgere.
5. **Deliberazione CdA del 27 dicembre 2004, n. 35** "*Decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali) – Documento programmatico della sicurezza – Approvazione*". Adozione da parte del Titolare del trattamento di un documento programmatico della sicurezza (art. 33 d.lgs. 196/2003).
6. **Deliberazione CdA del 13 aprile 2005, n. 5** "Deliberazione n. 18 del 28 giugno 2004 "Decreto legislativo 30 giugno 2003, n. 196 *(Codice in materia di protezione dei dati personali)* – Ex artt. 28 e 29 - Nomina dei Responsabili trattamento dati personali - Istruzioni" – Modifiche ed integrazioni", con la quale si procede alla nomina dei Responsabili esterni all'Agenzia e, specificatamente:
   a) ***Sigma Informatica S.p.A.***, per il pagamento delle indennità e rimborsi spese ai membri degli organi e del trattamento economico personale dipendente, convenzionato, a contratto;
   b) ***Monte dei Paschi di Siena S.p.A.***, per il pagamento delle indennità e rimborsi spese ai componenti degli organi e del trattamento economico personale dipendente, convenzionato e a contratto.
7. **Regolamento per il trattamento dei dati sensibili e giudiziari**. l'ARS ha partecipato al tavolo regionale per l'elaborazione del *"Regolamento per il trattamento dei dati sensibili e giudiziari di competenza della Regione, delle Aziende Sanitarie, degli Enti e Agenzie regionali, degli Enti vigilati dalla Regione"* approvato con DPGR 16 maggio 2006, n. 18/r.
8. **Deliberazione CdA del 3 aprile 2006, n. 7** concernente "Decreto legislativo 30 giugno 2003, n. 196 *(Codice in materia di protezione dei dati personali)* – Documento programmatico della sicurezza –Aggiornamento", con cui si è provveduto ad aggiornare il DPS in relazione ai mutamenti tecnologici ed organizzativi dell'Ente.
9. **Deliberazione CdA del 26 aprile 2007, n. 11** "Decreto legislativo 30 giugno 2003, n. 196 *(Codice in materia di protezione dei dati personali)* – Documento programmatico della sicurezza – Aggiornamento 2007", con cui si è provveduto ad apportare modifiche ed integrazioni al DPS approvato con deliberazione 7/2006, a seguito del mutato quadro istituzionale ed organizzativo introdotto con la novellata disciplina dell'ARS di cui alla l.r. 10 luglio 2006, n. 28 "*Modifiche alla legge regionale 24 febbraio 2005, n. 40 (Disciplina del servizio sanitario regionale) - Nuova disciplina dell'Agenzia regionale di sanità"* e ss.mm..
10. **Deliberazione CdA del 26 aprile 2007 n. 12,** con cui si sono apportate ulteriore modifiche ed integrazioni alla deliberazione 18/2004, sempre in conseguenza del novellato quadro istituzionale ed organizzativo dell'Ente;

11. **Determinazione n. 2 del Coord. Oss. Epidemiologia del 24 luglio 2007.** In qualità di "Responsabile esterno" del trattamento dei dati relativi all' "*Indagine Epidemiologica sullo stato di salute dell'Alta Val di Cecina",* all'uopo designata dal Titolare del trattamento dei dati dell'Azienda USL 5 - PISA[1], il Coordinatore, attraverso la determina *de qua*, ha anticipato la nomina dell'incaricato al trattamento dei dati per lo studio in parola, fornendo anche le istruzioni necessarie all'attività da svolgere.
12. **Determinazione n. 3 del Coord. Oss. Epidemiologia del 15 novembre 2007.** Per il trattamento di dati relativi all'*"Indagine concernente la revisione dei certificati di morte attinenti al registro e osservatorio di patologie",* il Coordinatore, attraverso la determina *de qua*, ha anticipato la nomina degli incaricati al trattamento dei dati per lo studio in parola, fornendo anche le istruzioni necessarie all'attività da svolgere.
13. **Istituzione del CE.TRA (Censimento dei trattamenti dei dati),** eseguiti da ARS per le attività di studio e ricerca alla stessa conferite dalla legge istitutiva; il CE.TRA rappresenta un modalità per attuare un costante monitoraggio del trattamento dei dati, utile anche ai fini dell'aggiornamento della *"Notificazione"* al Garante di cui al punto 2 che precede.
14. **Istituzione anagrafe dei responsabili/incaricati** per garantire l'effettivo esercizio dei diritti dell'interessato.
15. **Istituzione registro convenzioni/protocolli d'intesa/contratti** per monitorare i rapporti istaurati con altri enti ai fini del trattamento del dati in entrata/uscita da ARS.
16. **Apertura del portale "Privacy",** in fase di allestimento, per favorire la più ampia trasparenza e correttezza nei confronti degli utenti.

Il presente documento è strutturato in modo tale da essere diviso per Capitoli, articolati a loro volta in paragrafi, preceduti dalla presente premessa in cui sono state esplicitate:

- le finalità e gli obiettivi del documento;
- le azioni poste in essere dall'ARS in adempimento alla disciplina recata dal "Codice";
- le azioni in corso di definizione.

- ***Il Cap. I,*** si prefigge lo scopo di illustrare i principi e le regole generali per il trattamento dei dati personali, specificatamente, di quelli sensibili e giudiziari, delineando, per sommi capi, le attività rilevanti che derivano dall'applicazione del "Codice" e le conseguenze della violazione o mancato adempimento delle disposizioni ivi contenute. Lo scopo è anche quello di offrire un quadro generale degli adempimenti in capo anche ad altri enti del sistema socio sanitario con i quali l'Agenzia instaura contatti per l'esercizio delle funzioni istituzionali, pur avendo gli stessi natura giuridica e finalità istitutiva diverse da quelle di ARS.

- ***Nel Cap. II,*** si affrontano gli obblighi che derivano ad ARS, a seconda della veste formale con cui agisce, in applicazione della normativa in materia di privacy; specificatamente:
  - gli obblighi a rilevanza esterna da attuare verso il Garante;

[1] *Nota Azienda USL 5 di Pisa - Prot. 2540 del 16 gennaio 2007.*

- gli obblighi a rilevanza interna in attuazione delle disciplina recata dal nuovo "Codice Privacy";
- gli strumenti posti in essere per il coordinamento, il monitoraggio, l'aggiornamento delle azioni realizzate in attuazione delle disposizioni sulla riservatezza;
- l'apertura di un portale "Privacy, per adempiere agli obblighi di trasparenza sanciti dal "Codice".

- *Il Cap. III*, in ultimo, affronta il tema degli incaricati e, specificatamente:
  - del loro ruolo;
  - del profilo di autorizzazione assegnato a ciascun operatore secondo quanto indicato con deliberazione del CdA n. 18/2004 e ss.mm.;
  - delle modalità per la loro nomina;
  - delle prescrizioni generali cui gli incaricati devono attenersi nel trattamento di dati personali;
  - delle prescrizioni specifiche strettamente correlate al profilo di autorizzazione cui gli incaricati devono obbligatoriamente attenersi, articolate per tipologia di strutture: scientifica e tecnico-amministrativa.

Per facilitarne la reperibilità il testo del presente documento è disponibile sul sito web dell'ARS, selezionale la voce *"Portale Privacy".*

Firenze, 29 febbraio 2008

IL COORDINATORE
RESPONSABILE DEL TRATTAMENTO DEI DATI SENSIBILI
DELL'OSSERVATORIO DI EPIDEMIOLOGIA

_____

IL COORDINATORE
RESPONSABILE DEL TRATTAMENTO DEI DATI SENSIBILI
DELL'OSSERVATORIO PER LA QUALITA'

_____

IL DIRETTORE
RESPONSABILE DEL TRATTAMENTO DEI DATI SENSIBILI E
GIUDIZIARI DELLA DIREZIONE

_____

CAPITOLO I

REGOLE GENERALI

CAPITOLO I
REGOLE GENERALI

1.1 Definizioni

Si riportano di seguito, al fine di facilitare la comprensione del testo, alcune definizioni principali come disciplinate dall'art. 4 del "Codice"; le stesse sono raggruppate per voci: *dati, operazioni, soggetti e misure di sicurezza,* per consentirne una più agevola consultazione::

1.1.1 Dati

Si intende per:

a) ***"dato personale",*** qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

b) all'interno di questa definizione più generale si specificano ulteriore tipologie di dati ***"dati identificativi"*** che sono i dati personali che permettono l'identificazione diretta dell'interessato.-
Un soggetto s'intende identificabile quando è possibile associare le informazioni ai dati identificativi del soggetto, attraverso l'impiego di mezzi ragionevoli.

Il Codice inoltre identifica ***i dati sensibili***, ***i dati giudiziari***, ***gli altri dati particolari***, i dati così detti ***comuni***. Tale classificazione è definita in relazione al diverso livello di riservatezza proprie delle varie tipologie dei dati, delle diverse precauzioni che la legge richiede per il loro utilizzo, per la loro custodia e per il loro trattamento e della oggettiva diversa pericolosità per l'individuo derivante da un illecito trattamento.

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 od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;***"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";***"altri dati particolari".*** Un'ulteriore categorie di dati è quella prevista dall'art. 17 del Codice, intermedia tra dati sensibili e comuni, il cui trattamento presenta rischi specifici per i diritti, le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può determinare. Il loro trattamento è ammesso nel rispetto di misure e accorgimenti a garanzia dell'interessato ove prescritti dal Garante;***dati personali comuni,*** i dati che per semplicità sono definiti tali e

corrispondono a tutti i restanti dati personali, non compresi nelle precedenti categorie es.: dati anagrafici, coordinate bancarie, codice fiscale); ***"dato anonimo"*** il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile".Operazioni

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;

Nell'ambito delle varie fasi del trattamento particolare attenzione è riservata dalla legge a quelle relative alla ***comunicazione*** e alla ***diffusione*** cui viene attribuito il seguenti significato:

b) per ***"comunicazione"*** s'intende 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;

c) per ***"diffusione"*** s'intende il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

1.1.3 Soggetti

Il trattamento dei dati è ammesso solo da parte del Titolare dei dati, dei Responsabili del trattamento dei dati e degli incaricati, con attribuzione di compiti e responsabilità a questi soggetti, in relazione al ruolo da essi svolto nell'ambito del trattamento.

a) ***"Titolare",*** la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;

b) ***"Responsabile"***, la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;

c) ***"Incaricati",*** le persone fisiche autorizzate per iscritto dal titolare o dal responsabile a compiere operazioni di trattamento, cioè che effettuano materialmente le operazioni di trattamento, che devono essere eseguite secondo le modalità contemplate nel presente documento attenendosi al profilo assegnato. Possono essere individuati incaricati solo le persone fisiche;

d) ***"Interessato",*** la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;

e) ***"Garante",*** l'autorità di cui all'articolo 153, istituita dalla legge 31 dicembre 1996, n. 675.

1.1.4 Misure di sicurezza

Le misure di sicurezza sono articolate in due gruppi correlati. Il primo inserito nel corpo del Codice agli articoli 31, 32, 33, 34, 35 e 36; il secondo riportato in allegato. *Allegato B*, o "*Disciplinare tecnico*", composto da 29 dettagliate prescrizioni. S'intende per:

a) *"**misure minime***", il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31 del Codice;
b) ***"misure idonee",*** le misure volte a prevenire l'eventuale distruzione, dispersione o accesso non autorizzato ai documenti. Rispetto alle disposizioni contenute nel d.p.r. n. 318/99, il sistema delle misure minime di sicurezza viene semplificato e aggiornato sulla base dell'esperienza applicativa acquisita e dell'evoluzione tecnologica. In particolare, ai fini dell'applicazione delle misure minime richieste, si conferma la separazione tra trattamenti effettuati con "*strumenti elettronici"* e trattamenti *"cartacei"* senza che vi sia l'ulteriore distinzione tra trattamenti effettuati con elaboratori accessibili da altri elaboratori o terminali e trattamenti con elaboratori accessibili in rete.
c) ***"strumenti elettronici"***, gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;
c) ***"autenticazione informatica"***, l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;
d) ***"credenziali di autenticazione"***, i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;
e) ***"parola chiave",*** componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;
f) ***profilo di autorizzazione"***, l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;
g) ***"sistema di autorizzazione",*** l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.
f) ***"blocco"*** la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;
g) *"**banca di dati**"* qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti.

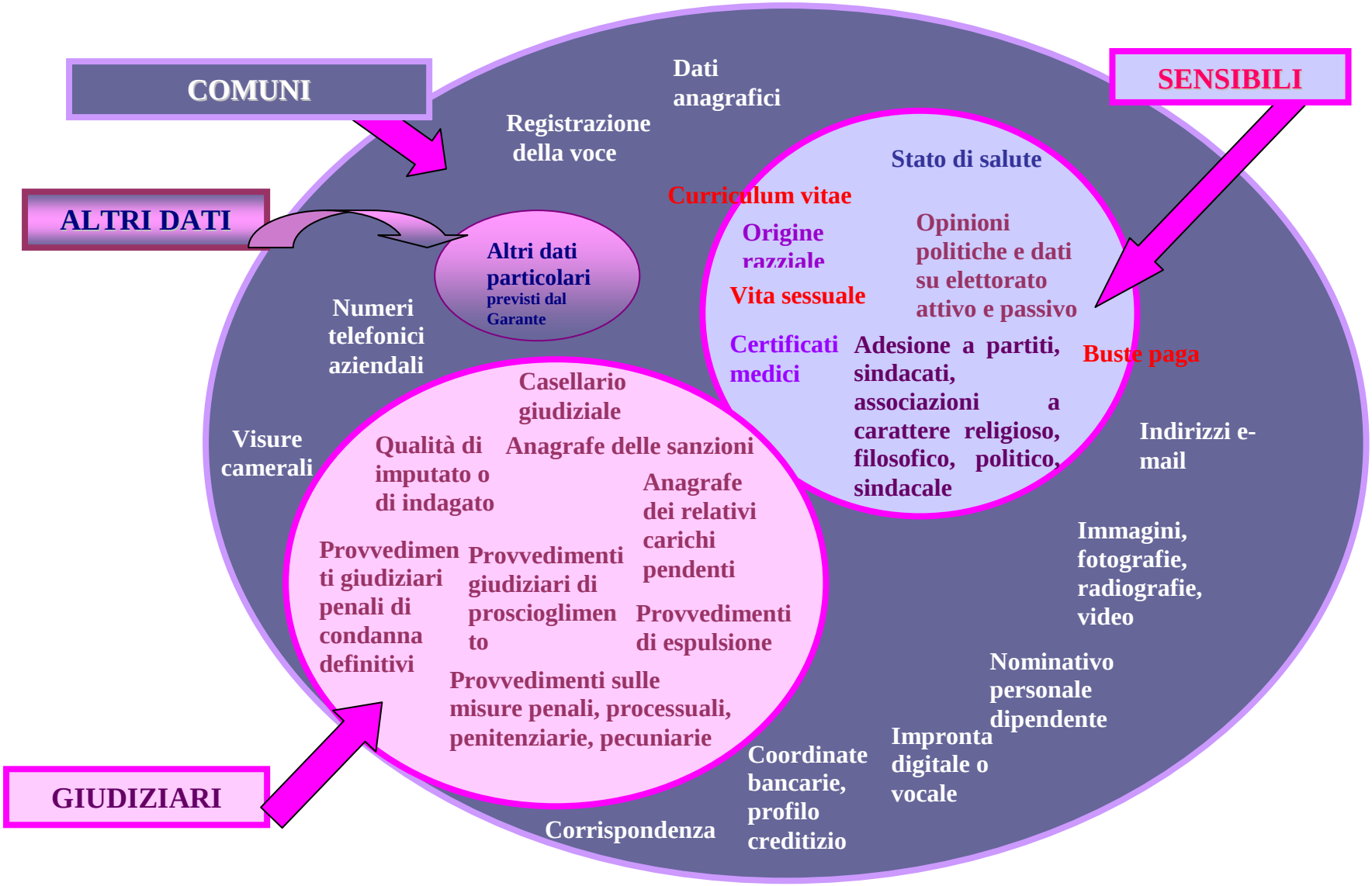
Ai fini del "Codice" si intende, altresì, per:

a) ***"scopi storici",*** le finalità di studio, indagine, ricerca e documentazione di figure, fatti e circostanze del passato;
b) ***"scopi statistici",*** le finalità di indagine statistica o di produzione di risultati statistici, anche a mezzo di sistemi informativi statistici;

c) ***"scopi scientifici"***, le finalità di studio e di indagine sistematica finalizzata allo sviluppo delle conoscenze scientifiche in uno specifico settore.

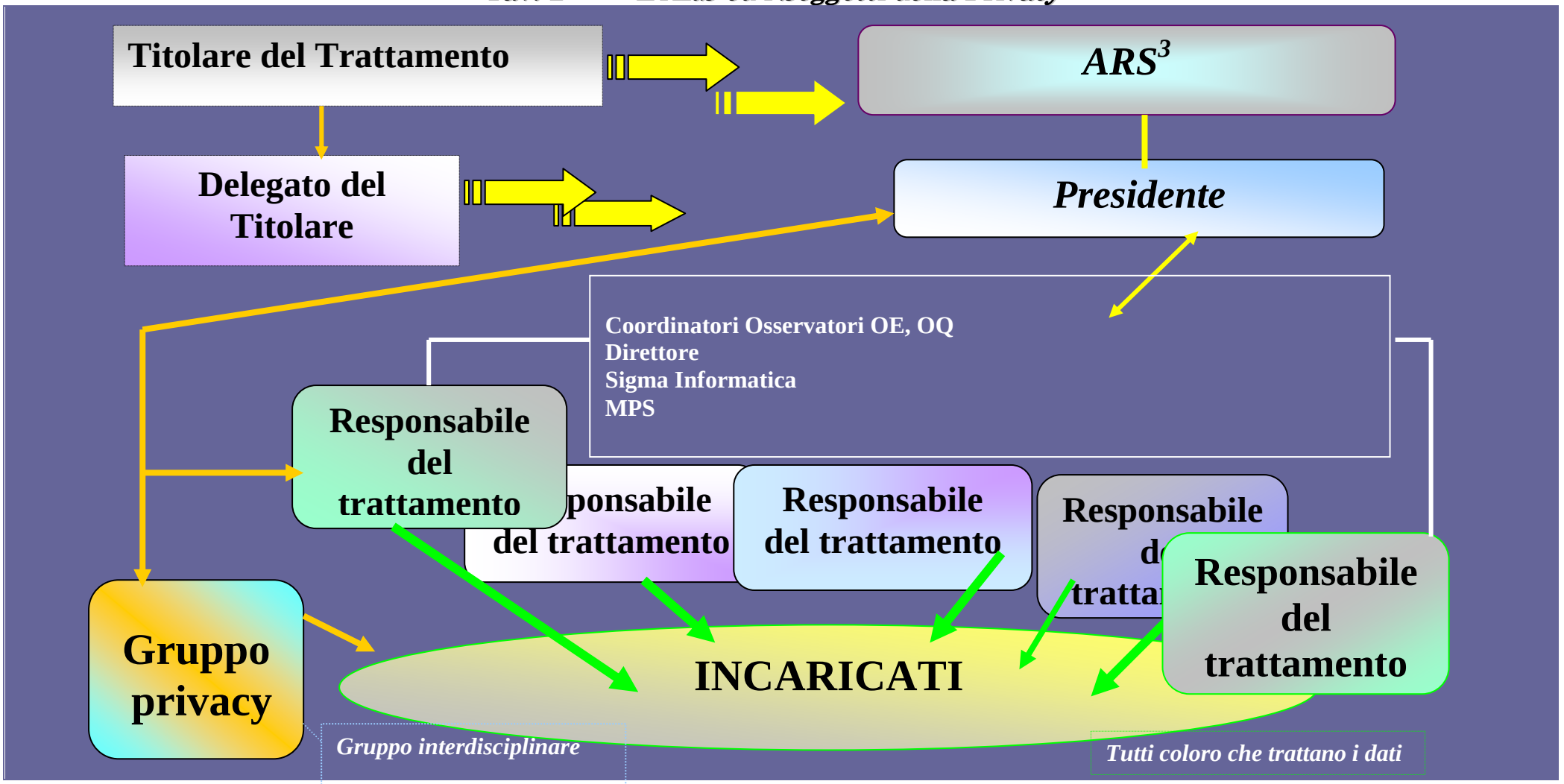
Si vedano al riguardo gli schemi che seguono che riassumono graficamente le tipologie dei dati, ***(Tav. 1)*** e, per ciò che concerne i "soggetti" della privacy, l'assetto organizzativo di ARS ***(Tav. 2):***

Tav. 1 –Schema riassuntivo dei dati personali[2]



2 Il Codice definisce dato personale "…qualunque informazione relativa a persona fisica o giuridica, ente o associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale". I dati identificativi sono i dati personali che permettono l'identificazione diretta dell'interessato, mentre quelli identificabili sono i dati personali che consentono l'identificazione del soggetto indirettamente, attraverso cioè l'incrocio con altri dati.

Tav. 2 "L'ARS ed i Soggetti della Privacy "



3 ARS è titolare dei trattamenti dei dati inerenti le attività di studio e ricerca dalla stessa individuate per l'esercizio delle funzioni istituzionali.

1.2 Nozioni generali

Il testo unico in materia di protezione dei dati personali, definitivamente approvato dal Consiglio dei ministri il 27 giugno 2003, ha assunto la veste giuridica di "Codice" *(Decreto legislativo 30 giugno 2003, n. 196, pubblicato in G.U. 29 luglio 2003, Serie generale n. 174, Supplemento ordinario n. 123/L),* di seguito denominato "Codice" o "Codice della privacy*".* Questa peculiare denominazione indica, oltre che l'importanza della normativa in parola, anche la circostanza che il Codice, recependo le direttive comunitarie, riunisce e coordina - in unico testo - la "vecchia" legge 675/1996 e gli altri decreti legislativi, regolamenti e codici deontologici che si erano succeduti dalla data dell'introduzione di tale legge, procedendo contestualmente alla loro abrogazione.
Il Codice della privacy ha altresì innovato in materia di riservatezza nelle comunicazioni elettroniche, raccogliendo alcuni spunti tratti sia da precedenti decisioni, pareri, segnalazioni del Garante, sia dalla direttiva UE 2000/58.
Il Codice è diviso in tre parti:

- **la prima** dedicata alle disposizioni generali, riordinate in modo tale da trattare tutti gli adempimenti e le regole del trattamento con riferimento ai settori pubblico e privato;
- **la seconda** è la parte speciale dedicata a specifici settori: questa sezione, oltre a disciplinare aspetti in parte inediti (informazione giuridica, notificazioni di atti giudiziari, dati sui comportamenti debitori), completa anche la disciplina attesa da tempo per il settore degli organismi sanitari e quella dei controlli sui lavoratori;
- **la terza** affronta la materia delle tutele amministrative e giurisdizionali con il consolidamento delle sanzioni amministrative e penali e con le disposizioni relative all'Ufficio del Garante.
- Il "Codice" si completa con:
  - **Tavola di corrispondenza** dei riferimenti previgenti al codice in materia di protezione dei dati personali;
  - **ALLEGATI** :
    - Codici di Deontologia (Allegato A)
      A.1 - Trattamento di dati personali nell'esercizio dell'attività giornalistica
      A.2 - Trattamento di dati personali per scopi storici
      A.3 - Trattamento di dati personali per scopi statistici in ambito SISTAN;
    - Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B):
    - Trattamenti non occasionali effettuati in ambito giudiziario o per fini di polizia - Artt. 46 e 53 del codice (Allegato C)
  - **Indice alfabetico**

In questo quadro, particolare rilevanza assume la figura del "Garante", organo collegiale indipendente, istituito dalla legge 675/1996 che, in virtù della sua posizione di terzietà ed imparzialità, è in grado di assicurare il rispetto delle garanzie di tutela della sfera privata del cittadino da parte di terzi o della Pubblica Amministrazione.
La funzione essenziale di tale Authority è quella di verificare se la gestione dei dati avviene in conformità con quanto dichiarato e nel rispetto della tutela della privacy.

Procedendo ad un esame più dettagliato della nuova disciplina sulla privacy, è agevole raggruppare la medesima in tre fondamentali componenti; specificatamente:

1. *le disposizioni generali* (articoli da 1 a 45), riguardanti le regole sostanziali della disciplina del trattamento dei dati personali, applicabili a tutti i trattamenti, nonché le regole specifiche che si devono osservare per i trattamenti effettuati da soggetti pubblici e quelle che trovano applicazione per i trattamenti effettuati da soggetti privati e da enti pubblici economici;
2. *le disposizioni particolari*, che si applicano a determinati settori (articoli da 46 a 140); oltre a disciplinare aspetti specifici ad integrazione o eccezione delle disposizioni generali, contenute nella Prima parte, introducono la disciplina per il settore sanitario e quella dei controlli sui lavoratori;
3. *le disposizioni in materia di tutela amministrativa e giurisdizionale* (articoli da 141 a 152), le disposizioni che regolano l'Ufficio del Garante (articoli da 153 a 160), il consolidamento delle sanzioni amministrative e penali (articoli da 161 a 172), cui si aggiungono le norme di modifica, finali e di carattere transitorio (articoli da 173 a 186).

Le disposizioni contenute nel Codice, in estrema sintesi, disciplinano le modalità di uso dei dati personali e, prescrivendo forme di tutela del diritto alla riservatezza, definiscono i meccanismi di controllo e le misure sanzionatorie.

In altri termini, l'obiettivo che la nuova disciplina si propone non è quello di impedire la circolazione delle informazioni personali – questo si tradurrebbe in una limitazione alla libertà d'informazione - bensì è quello di regolamentare il trattamento dei dati personali e, specificatamente di quelli sensibili e giudiziari, assicurando trasparenza ed evitando la lesione di diritti degli interessati.

Per tali ragioni la normativa impone l'obbligo di informare il soggetto nei cui confronti si raccolgono i dati delle modalità con cui tale attività avviene e delle finalità del loro utilizzo. Ed è per le stesse ragioni che la legge vuole che, prima di utilizzare i dati personali di un soggetto, si raccolga, in taluni casi, il suo consenso; per altri, viceversa, si può procedere con un'informativa di dettaglio. Deroghe specifiche, infatti, sono autorizzate, su questo tema, per le Pubbliche Amministrazioni (si veda appunto l'ARS).

In estrema sintesi è bene evidenziare quelli che sono i principi fondamentali enucleati dal Codice in materia di trattamento di dati sensibili:

- **il diritto alla protezione**: per cui chiunque ha diritto alla tutela dei dati personali che lo riguardano;
- **le finalità**: il Codice garantisce che il trattamento di dati si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, assicurando un elevato livello di protezione, nel rispetto dei principi di semplificazione,armonizzazione ed efficacia delle modalità previste per il loro esercizio;
- **la necessità del trattamento dei dati**: viene sancito che i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzo di dati personali ed identificativi, escludendone addirittura il trattamento e, laddove sia possibile, impone l'utilizzo di dati anonimi o che permettano l'identificazione solo in caso di necessità (art. 3).

  Quest'ultimo principio non ha precedenti nella disciplina previgente, quindi rappresenta un'assoluta novità del Codice, che ha ravvisato nell'anonimato lo strumento più idoneo a garantire la tutela della riservatezza.

  I dati personali oggetto di trattamento devono essere custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo,

mediante l'adozione di idonee e preventive misure di sicurezza, i rischi, anche accidentali, di distruzione o perdita dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Regole generali per il trattamento dei dati personali sono descritte nel Titolo III della Parte I del Codice, ove si afferma che il trattamento di cui trattasi debba avvenire secondo i principi di liceità, correttezza, esattezza e pertinenza e sia compatibile agli scopi prefissati, eccezion fatta per la predisposizione di alcune cautele per i trattamenti particolarmente rischiosi.

Riassumendo, i dati personali e specificatamente quelli sensibili e giudiziari, oggetto di trattamento devono essere:

a) **trattati in modo lecito e secondo correttezza;**
b) **raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;**
c) **esatti e, se necessario, aggiornati;**
d) **pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;**
e) **conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.**

Per quel che rileva ai fini della presente trattazione, l'attenzione si focalizza sul capo II del Titolo III della Parte I del Codice, ove sono disciplinati i trattamenti effettuati da soggetti pubblici, esclusi gli enti pubblici economici.

Tenendo per il momento da parte gli esercenti le professioni sanitarie e gli organismi sanitari pubblici, per i quali è prevista una disciplina *ad hoc* nonché i trattamenti relativi ai dati sensibili e giudiziari, il Codice pone come prima regola la necessità che il trattamento avvenga esclusivamente per fini istituzionali.

La normativa sulla privacy dichiara consentito per i **soggetti pubblici** qualunque trattamento dei dati personali effettuato **per lo svolgimento delle funzioni istituzionali**, nei limiti stabiliti dal Codice, dalle leggi e dai regolamenti, e l'ente **non ha l'obbligo di richiedere il consenso** all'interessato, poiché tali funzioni sono svolte nell'interesse della collettività sulla base di norme che definiscono i suoi compiti istituzionali.

Qualora fossero trattati dati senza l'autorizzazione, anche con il consenso dell'interessato, non potrebbero comunque essere trattati; in tal caso, **il consenso non avrebbe alcun valore in quanto non necessario e non richiesto per la P.A.**.

Il Codice fornisce una disciplina diversa a seconda dei tipi di dati trattati, ad esempio, nel caso dei dati non sensibili e non giudiziari, i dati comuni, il trattamento è consentito per lo svolgimento delle funzioni istituzionali **anche in assenza di norma di legge o regolamento**, tranne che per la comunicazione e la diffusione ai soggetti privati, per le quali vige una riserva di legge, il che significa che il trattamento di tali dati è possibile **solo** in presenza di una disposizione di legge che lo preveda.

In particolare, negli articoli da 18 a 22, detta alcune disposizioni specifiche che si affiancano a quelle di generale applicazione relative all'adozione delle misure minime di sicurezza, fra cui il Documento programmatico sulla sicurezza (DPS), al quale sono tenute, se ve ne sono i presupposti relativamente al trattamenti effettuati, anche le P.A.

Nello specifico, l'articolo 18 esenta i soggetti pubblici (con esclusione di quelli economici) dal richiedere il consenso dell'interessato per il trattamento dei dati personali, che però potrà essere effettuato esclusivamente per lo svolgimento delle funzioni istituzionali.

A condizione che rientri in tali funzioni, il trattamento di dati diversi da quelli sensibili e giudiziari è consentito anche in mancanza di una norma di legge o di regolamento che lo preveda espressamente.
Appare interessante evidenziare che la differenza esistente fra le operazioni della **comunicazione** e della **diffusione** risiede nella determinatezza dei soggetti, a cui si rivolge la prima, rispetto all'indeterminatezza dei soggetti destinatari della seconda.
La comunicazione dei dati personali ad altri soggetti pubblici, se necessaria per lo svolgimento delle funzioni istituzionali, è consentita **anche in assenza di una norma di legge o regolamento**, in tal caso però il Codice prevede di darne comunicazione al Garante[2] ai fini della verifica del rispetto della disciplina vigente e, secondo una delle novità introdotte dal Codice, occorre attendere il termine di 40/45 giorni dalla comunicazione al Garante prima di poter trasmettere ai soggetti pubblici tali dati.
Nel caso di **dati sensibili e giudiziari** il Codice presenta una disciplina più rigida, anche se poi il Garante, per alleggerire gli oneri che incombono su coloro che debbono trattare i dati per l'esercizio delle funzioni istituzionali, è intervenuto adottando una serie di autorizzazioni generali (vedasi Cap. II).
Il trattamento di tali tipi di dati da parte di soggetti pubblici è consentito nei seguenti casi:

1. trattamento autorizzato da un'espressa disposizione di legge (o anche da un provvedimento del Garante, nel caso dei dati giudiziari) che specifica le finalità di rilevante interesse pubblico perseguite, i tipi di dati che possono essere trattati e i tipi di operazioni eseguibili;
2. esistenza di una disposizione di legge che specifichi solo la finalità di interesse pubblico, quando il soggetto che effettua il trattamento abbia identificato, con proprio regolamento, i tipi di dati e di operazioni indispensabili per lo svolgimento, nel caso specifico, delle proprie attività istituzionali;
3. trattamenti per lo svolgimento di attività istituzionali per cui non sia stata prevista né la finalità di rilevante interesse pubblico né i tipi di dati, né le operazioni eseguibili. In questo caso dovrebbe essere richiesto al Garante il riconoscimento della rilevante finalità di interesse pubblico per le attività svolte, dopodichè regolamentare i tipi di dati e le operazioni eseguibili. Rispetto alla recedente formulazione, il Codice ha stabilito che la identificazione dei tipi di dati e di operazioni indispensabili per il perseguimento delle finalità di rilevante interesse pubblico debba essere fatta dal titolare con atto di natura regolamentare e che tale atto deve essere adottato in conformità al parere espresso dal Garante, anche in base a modelli standard.
4. E' stato differito il termine di adozione del regolamento sui dati sensibili e giudiziari. Il decreto legge pubblicato nella Gazzetta Ufficiale del 28/12/2006, n. 300, ha differito al 28 febbraio 2007 il termine di adozione di tale regolamento da parte di soggetti pubblici.[3]

[2] La comunicazione è prevista per le circostanze di cui all'art. 39, cioè relativamente al trattamento di dati idonei a rilevare lo stato di salute della popolazione previsti dai programmi di ricerca biomedica e sanitaria di cui all'art. 12- bis d.lgs. 502/1992 e succ. modif. (cfr. art. 39, c.1 lett. b) Codice") e relativamente alla comunicazione dei dati personali da parte di un soggetto pubblico all'ARS e viceversa, non previsto da norma di legge o regolamento, effettuata in qualunque forma anche mediante convenzione (cfr. art. 39, comma 1, lett. a) "Codice"). La comunicazione è inviata utilizzando il modello che dovrà essere predisposto dal Garante, **non ancora reso disponibile**.

[3] La Regione ha già provveduto con DPGR del 16 maggio 2006, n. 18/r, come precisato al successivo par. 2.3.1.

Per ciò che concerne l'Agenzia, definita dalla legge istitutiva ente avente natura giuridica pubblica, si fa espresso riferimento a quanto riportato nel Cap. II, par. 2.3.1

Nel tessuto normativo del Codice si possono individuare alcuni adempimenti che riguardano sia i soggetti pubblici che i soggetti privati:

- l'individuazione del titolare;
- la designazione dei responsabili dei trattamenti;
- la nomina degli incaricati;
- la notificazione al Garante, se dovuta ai sensi dell'art. 37 del Codice;
- il rispetto delle modalità generali per il trattamento dei dati e delle disposizioni contenute nei codici deontologici, per quanto di competenza;
- l'informativa/consenso[4] agli interessati (che però, nel caso di trattamento di dati sensibili e giudiziari, deve contenere anche l'espresso riferimento alla normativa che prevede gli obblighi o i compiti in base ai quali è effettuato il trattamento);
- l'adozione di idonee misure per agevolare l'esercizio dei diritti da parte dell'interessato;
- la redazione del documento programmatico per la sicurezza e l'adozione delle misure minime di sicurezza.

1.3 Attività rilevanti

Per attività rilevanti si intendono l'insieme di tutti quegli adempimenti, che il Codice richiede per attuare le prescrizioni. In particolare, il d.lgs. n. 196/2003 contiene una serie di disposizioni relative al trattamento dei dati personali da parte dei soggetti pubblici. E' necessario distinguere tra:

- **trattamento;**
- **notificazione;**
- **autorizzazione;**
- **consenso/informativa**
- **comunicazione;**
- **raccolta;**
- **diffusione.**

Rinviando alla disamina di dettaglio contenuta nel Cap. II che affronta gli obblighi di ARS relativamente alle attività sopra identificate, si ritiene opportuno, in questa sede, sintetizzare, sul piano generale, i concetti sopra elencati, al fine di offrire un quadro generale di conoscenze utile anche per l'instaurazione di rapporti con altri enti del sistema sanitario e socio-sanitario.

- **Trattamento,** per il cui significato si fa rinvio a quanto precisato al precedente paragr. 1.1.
- La **notificazione,** consiste nella dichiarazione con la quale un soggetto pubblico o privato rende nota al Garante per la protezione dei dati personali l'esistenza di un'attività di raccolta e utilizzazione dei dati personali, svolta quale autonomo Titolare del trattamento (art. 37 Codice).

[4] Per quanto riguarda ARS si fa espresso riferimento al Cap. II, paragr. 2.3.3.

- L'**autorizzazione** è rilasciata dal Garante per determinate tipologie di dati, permettendo ai destinatari il loro trattamento.
- Il **Consenso/Informativa**. Il disposto di cui all'art. 18, comma 4 chiarisce che i soggetti pubblici, nello svolgimento delle funzioni istituzionali, non debbano richiedere il consenso dell'interessato per la raccolta e il trattamento dei dati, salvo i casi espressamente previsti dal Codice che tuttavia non sono riconducili ad ARS come precisato al successivo paragr. 2.3.3.
  L'informativa, viceversa, è sempre dovuta.

Limiti incontrano invece la comunicazione, la diffusione e la notificazione: tali limiti differiscono a seconda del soggetto (pubblico o meno) che riceve la comunicazione e/o la diffusione dei dati da parte dell'ente pubblico titolare del trattamento; l'obbligo di notificazione varia a seconda della natura del dato trattato.

- La **comunicazione** consiste nel dare conoscenza dei dati personali a uno o più soggetti determinati, diversi dall'interessato in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
- La **raccolta,** per raccolta dati si intende l'operazione o complesso di operazioni attraverso le quali il dato è tratto da un soggetto e immesso in una banca dati o presso qualsiasi complesso organizzato, ripartito in una o più unità dislocate in uno o più siti; in generale il trattamento del dato inizia con la raccolta dello stesso.
- La **diffusione** consiste nel dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Si ritiene utile, in ultimo, dare alcune delucidazioni di carattere generale sul trattamento **dei dati personali che non siano né dati sensibili né giudiziari**. Lo schema, che segue, ***Tab. 1***, rappresenta una sintesi della disciplina recata dall'art. 19 del Codice:

Tab. 1 – Trattamento dati comuni (sintesi disciplina art. 19 Codice)

Tipo di operazione	Verso soggetti pubblici	Verso privati o enti pubblici economici
Raccolta	libera	libera
Trattamento	libero	libero
Trasferimento/Comunicazione di dati	**Sono consentiti**: · se previsti da norme di legge o di regolamento · se necessari per lo svolgimento delle funzioni Istituzionali, ma PREVIA comunicazione al Garante e TRASCORSI 45 giorni dalla comunicazione senza che sia pervenuta una diversa determinazione dello stesso.	Sono consentiti se previsti da norma di legge o regolamento
Diffusione	E' consentita se prevista da norma di legge o regolamento	E' consentita se prevista da norma di legge o regolamento

1.4 Sanzioni

Sanzioni pecuniarie e penali sono aumentate per chi viola la privacy, in particolare per l'uso dei dati senza consenso degli interessati, per il mancato adempimento degli obblighi verso il Garante o nei confronti di un provvedimento dello stesso, per la mancata informativa agli interessati sull'uso che si intende fare dei dati che li riguardano.
Il trattamento dei dati personali è, infatti, equiparato ad attività pericolosa (art. 15, c. 1), ai sensi dell'art. 2050 del codice civile. In base a detta norma il titolare sarà tenuto a risarcire i danni, a meno che non provi ad aver adottato le misure "idonee" (non solo le minime) per evitare il danno.
La novità è nel secondo comma dell'art. 15 secondo cui il danno non patrimoniale è risarcibile anche in caso di violazione delle norme attinenti alle modalità del trattamento comprendenti anche le regole sulla conservazione. Di conseguenza, chi trattando dati personali provoca danni è tenuto al risarcimento.
Le tabelle che seguono, ***Tab. 2 e Tab. 3,*** riassumono rispettivamente gli illeciti civili e penali e le relative sanzioni pecuniarie e penali comminate in caso di inadempienza o violazione:

Tab. 2

ILLECITI CIVILI - VIOLAZIONI AMMINISTRATIVE	
Violazione	***Sanzione***
Art. 161 Assenza informativa privacy Assenza informativa privacy per dati sensibili o giudiziari o in caso di trattamenti che presentano rischi specifici o di maggiore rilevanza del pregiudizio	▪ Sanzione da 3.000 a 18.000 euro. ▪ Sanzione da 5.000 a 30.000 euro. (moltiplicabile per 3 a seconda delle condizioni economiche del contravventore).
Art. 162 Altre fattispecie Cessione dei dati in violazione di quanto previsto dall'articolo 16, comma 1, lettera b)[5] o di altre disposizioni in materia di disciplina del trattamento La violazione della disposizione di cui all'articolo 84, comma 1[6]	▪ Sanzione amministrativa del pagamento di una somma da 5.000 euro a 30.000 euro. ▪ Sanzione amministrativa del pagamento di una somma da 500 euro a 3.000 euro.
163. Omessa o incompleta notificazione.	▪ Sanzione amministrativa del pagamento di una somma da 10.000 a 60.000 euro e con la sanzione amministrativa accessoria della pubblicazione dell'ordinanza-ingiunzione, per intero o per estratto, in uno o più giornali indicati nel provvedimento che la applica.
164. Omessa informazione o esibizione al Garante. Omissione di fornire le informazioni o di esibire i documenti richiesti dal Garante ai sensi degli articoli 150, comma 2[7], e 157[8]	▪ Sanzione amministrativa del pagamento di una somma da 4.000 euro a 24.000 euro
165. Pubblicazione del provvedimento del Garante. Nei casi di cui agli articoli 161, 162 e 164	▪ Può essere applicata la sanzione amministrativa accessoria della pubblicazione dell'ordinanza-ingiunzione, per intero o per estratto, in uno o più giornali indicati nel provvedimento che la applica.

[5] L'art. 16 recante "Cessazione del trattamento" prevede, al comma 1, lett. b) che in caso di cessazione, per qualsiasi causa, di un trattamento i dati che non siano stati distrutti o conservati per fini personali, devono essere ceduti ad altro titolare, purché destinati ad un trattamento in termini compatibili agli scopi per i quali i dati sono raccolti. Ne consegue, ai sensi della disposizione recata dall'art. 162, l'inosservanza dell'obbligo in parola è illecito amministrativo.

[6] L'art. 84, comma 1, stabilisce che i dati personali idonei a rivelare lo stato di salute possano essere resi noti da parte di esercenti le professioni sanitarie ed organismi sanitari all'interessato o, in caso di impossibilità di questo ultimo, ai soggetti di cui all'articolo 82, comma 2, lettera a), (cioè un prossimo congiunto, un familiare, un convivente o, in loro assenza, il responsabile della struttura presso cui dimora l'interessato), solo per il tramite di un medico designato dall'interessato o dal titolare; in caso di trasmissione di detti dati a soggetti diversi, scatta la sanzione.

[7] L'art. 150, comma 1, prevede che, nel caso di ricorso al Garante, questo ultimo nel valutare la fondatezza dello stesso può assumere dagli interessati le informazioni necessarie alla maturazione del proprio convincimento. L'omissione da parte dei destinatari della richiesta delle informazioni è sanzionata.

[8] L'art. 157 stabilisce che per l'espletamento dei propri compiti il Garante possa richiedere al titolare, al responsabile, all'interessato o anche a terzi di fornire informazioni e di esibire documenti; la mancata risposta da parte di tali soggetti è sanzionata.

Tab. 3

ILLECITI PENALI	
Illecito	***Sanzioni penali***
167. Trattamento illecito di dati. Chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 18, 19, 23, 123, 126 e 130, ovvero in applicazione dell'articolo 129[9] Chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 17, 20, 21, 22, commi 8 e 11, 25, 26, 27 e 45[10].	▪ Se dal fatto deriva nocumento, reclusione da 6 a 18 mesi; ▪ se il fatto consiste nella comunicazione o diffusione, reclusione da 6 a 24 mesi. ▪ Se dal fatto deriva nocumento, reclusione da 1 a 3 anni
168. Falsità nelle dichiarazioni e notificazioni al Garante. Chiunque, nella notificazione di cui all'articolo 37 o in comunicazioni, atti, documenti o dichiarazioni resi o esibiti in un procedimento dinanzi al Garante o nel corso di accertamenti, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi.	▪ Salvo che il fatto costituisca più grave reato, reclusione da 6 mesi a 3 anni.

[9] L'**art. 18** .recante "Principi applicabili a tutti i trattamenti effettuati da soggetti pubblici" prevede:
"1. Le disposizioni del presente capo riguardano tutti i soggetti pubblici, esclusi gli enti pubblici economici. 2. Qualunque trattamento di dati personali da parte di soggetti pubblici è consentito soltanto per lo svolgimento delle funzioni istituzionali. 3. Nel trattare i dati il soggetto pubblico osserva i presupposti e i limiti stabiliti dal presente codice, anche in relazione alla diversa natura dei dati, nonché dalla legge e dai regolamenti. 4. Salvo quanto previsto nella Parte II per gli esercenti le professioni sanitarie e gli organismi sanitari pubblici, i soggetti pubblici non devono richiedere il consenso dell'interessato. 5. Si osservano le disposizioni di cui all'articolo 25 in tema di comunicazione e diffusione".
L'**art. 19** recante "Principi applicabili al trattamento di dati diversi da quelli sensibili e giudiziari." prevede:
"1. Il trattamento da parte di un soggetto pubblico riguardante dati diversi da quelli sensibili e giudiziari è consentito, fermo restando quanto previsto dall'articolo 18, comma 2, anche in mancanza di una norma di legge o di regolamento che lo preveda espressamente. 2. La comunicazione da parte di un soggetto pubblico ad altri soggetti pubblici è ammessa quando è prevista da una norma di legge o di regolamento. 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 decorso il termine di cui all'articolo 39, comma 2, e non è stata adottata la diversa determinazione ivi indicata.3. La comunicazione da parte di un soggetto pubblico a privati o a enti pubblici economici e la diffusione da parte di un soggetto pubblico sono ammesse unicamente quando sono previste da una norma di legge o di regolamento".
L'**art. 23** recante "Consenso" prevede:
"1. Il trattamento di dati personali da parte di privati o di enti pubblici economici è ammesso solo con il consenso espresso dell'interessato. 2. Il consenso può riguardare l'intero trattamento ovvero una o più operazioni dello stesso. 3. Il consenso è validamente prestato solo se è espresso liberamente e specificamente in riferimento ad un trattamento chiaramente individuato, se è documentato per iscritto, e se sono state rese all'interessato le informazioni di cui all'articolo 13. 4. Il consenso è manifestato in forma scritta quando il trattamento riguarda dati sensibili".
L'**art. 123** recante "Dati relativi al traffico" prevede:
"1. I dati relativi al traffico riguardanti abbonati ed utenti trattati dal fornitore di una rete pubblica di comunicazioni o di un servizio di comunicazione elettronica accessibile al pubblico sono cancellati o resi anonimi quando non sono più necessari ai fini della trasmissione della comunicazione elettronica, fatte salve le disposizioni dei commi 2, 3 e 5. 2. Il trattamento dei dati relativi al traffico strettamente necessari a fini di fatturazione per l'abbonato, ovvero di pagamenti in caso di interconnessione, è consentito al fornitore, a fini di documentazione in caso di contestazione della fattura o per la pretesa del pagamento, per un periodo non superiore a sei mesi, salva l'ulteriore specifica conservazione necessaria per effetto di una contestazione anche in sede giudiziale. 3. Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico può trattare i dati di cui al comma 2 nella misura e per la durata necessarie a fini di commercializzazione di servizi di comunicazione elettronica o per la fornitura di servizi a valore aggiunto, solo se l'abbonato o l'utente cui i dati si riferiscono hanno manifestato il proprio consenso, che è revocabile in ogni momento. 4. Nel fornire l'informativa di cui all'articolo 13 il fornitore del servizio informa l'abbonato o l'utente sulla natura dei dati relativi al traffico che sono sottoposti a trattamento e sulla durata del medesimo trattamento ai fini di cui ai commi 2 e 3. 5. Il trattamento dei dati personali relativi al traffico è consentito unicamente ad incaricati del trattamento che operano ai sensi dell'articolo 30 sotto la diretta autorità del fornitore del servizio di comunicazione elettronica accessibile al pubblico o, a seconda dei casi, del fornitore della rete pubblica di comunicazioni e che si occupano della fatturazione o della gestione del traffico, di analisi per conto di clienti, dell'accertamento di frodi, o della commercializzazione dei servizi di comunicazione elettronica o della prestazione dei servizi a valore aggiunto. Il trattamento è limitato a quanto è strettamente necessario per lo svolgimento di tali attività e deve assicurare l'identificazione dell'incaricato che accede ai dati anche mediante un'operazione di interrogazione automatizzata. 6. L'Autorità per le garanzie nelle comunicazioni può ottenere i dati relativi alla fatturazione o al traffico necessari ai fini della risoluzione di controversie attinenti, in particolare, all'interconnessione o alla fatturazione".
L'**art. 126** recante "Dati relativi all'ubicazione." prevede:

"1. I dati relativi all'ubicazione diversi dai dati relativi al traffico, riferiti agli utenti o agli abbonati di reti pubbliche di comunicazione o di servizi di comunicazione elettronica accessibili al pubblico, possono essere trattati solo se anonimi o se l'utente o l'abbonato ha manifestato previamente il proprio consenso, revocabile in ogni momento, e nella misura e per la durata necessari per la fornitura del servizio a valore aggiunto richiesto. 2. Il fornitore del servizio, prima di richiedere il consenso, informa gli utenti e gli abbonati sulla natura dei dati relativi all'ubicazione diversi dai dati relativi al traffico che saranno sottoposti al trattamento, sugli scopi e sulla durata di quest'ultimo, nonché sull'eventualità che i dati siano trasmessi ad un terzo per la prestazione del servizio a valore aggiunto. 3. L'utente e l'abbonato che manifestano il proprio consenso al trattamento dei dati relativi all'ubicazione, diversi dai dati relativi al traffico, conservano il diritto di richiedere, gratuitamente e mediante una funzione semplice, l'interruzione temporanea del trattamento di tali dati per ciascun collegamento alla rete o per ciascuna trasmissione di comunicazioni. 4. Il trattamento dei dati relativi all'ubicazione diversi dai dati relativi al traffico, ai sensi dei commi 1, 2 e 3, è consentito unicamente ad incaricati del trattamento che operano ai sensi dell'articolo 30, sotto la diretta autorità del fornitore del servizio di comunicazione elettronica accessibile al pubblico o, a seconda dei casi, del fornitore della rete pubblica di comunicazioni o del terzo che fornisce il servizio a valore aggiunto. Il trattamento è limitato a quanto è strettamente necessario per la fornitura del servizio a valore aggiunto e deve assicurare l'identificazione dell'incaricato che accede ai dati anche mediante un'operazione di interrogazione automatizzata".

L'**art. 129** recante "Elenchi di abbonati" prevede:

"1. Il Garante individua con proprio provvedimento, in cooperazione con l'Autorità per le garanzie nelle comunicazioni ai sensi dell'articolo 154, comma 3, e in conformità alla normativa comunitaria, le modalità di inserimento e di successivo utilizzo dei dati personali relativi agli abbonati negli elenchi cartacei o elettronici a disposizione del pubblico, anche in riferimento ai dati già raccolti prima della data di entrata in vigore del presente codice. 2. Il provvedimento di cui al comma 1 individua idonee modalità per la manifestazione del consenso all'inclusione negli elenchi e, rispettivamente, all'utilizzo dei dati per le finalità di cui all'articolo 7, comma 4, lettera b), in base al principio della massima semplificazione delle modalità di inclusione negli elenchi a fini di mera ricerca dell'abbonato per comunicazioni interpersonali, e del consenso specifico ed espresso qualora il trattamento esuli da tali fini, nonché in tema di verifica, rettifica o cancellazione dei dati senza oneri".

L'**art. 130** recante "Comunicazioni indesiderate" prevede:

"1. L'uso di sistemi automatizzati di chiamata senza l'intervento di un operatore per l'invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale è consentito con il consenso dell'interessato. 2. La disposizione di cui al comma 1 si applica anche alle comunicazioni elettroniche, effettuate per le finalità ivi indicate, mediante posta elettronica, telefax, messaggi del tipo Mms (Multimedia Messaging Service) o Sms (Short Message Service) o di altro tipo. 3. Fuori dei casi di cui ai commi 1 e 2, ulteriori comunicazioni per le finalità di cui ai medesimi commi effettuate con mezzi diversi da quelli ivi indicati, sono consentite ai sensi degli articoli 23 e 24. 4. Fatto salvo quanto previsto nel comma 1, se il titolare del trattamento utilizza, a fini di vendita diretta di propri prodotti o servizi, le coordinate di posta elettronica fornite dall'interessato nel contesto della vendita di un prodotto o di un servizio, può non richiedere il consenso dell'interessato, sempre che si tratti di servizi analoghi a quelli oggetto della vendita e l'interessato, adeguatamente informato, non rifiuti tale uso, inizialmente o in occasione di successive comunicazioni. L'interessato, al momento della raccolta e in occasione dell'invio di ogni comunicazione effettuata per le finalità di cui al presente comma, è informato della possibilità di opporsi in ogni momento al trattamento, in maniera agevole e gratuitamente. 5. È vietato in ogni caso l'invio di comunicazioni per le finalità di cui al comma 1 o, comunque, a scopo promozionale, effettuato camuffando o celando l'identità del mittente o senza fornire un idoneo recapito presso il quale l'interessato possa esercitare i diritti di cui all'articolo 7. 6. In caso di reiterata violazione delle disposizioni di cui al presente articolo il Garante può, provvedendo ai sensi dell'articolo 143, comma 1, lettera b), altresì prescrivere a fornitori di servizi di comunicazione elettronica di adottare procedure di filtraggio o altre misure praticabili relativamente alle coordinate di posta elettronica da cui sono stati inviate le comunicazioni".

[10] L'**art. 17** recante "Trattamento che presenta rischi specifici" prevede:

"1. Il trattamento dei dati diversi da quelli sensibili e giudiziari che presenta rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può determinare, è ammesso nel rispetto di misure ed accorgimenti a garanzia dell'interessato, ove prescritti.2. Le misure e gli accorgimenti di cui al comma 1 sono prescritti dal Garante in applicazione dei principi sanciti dal presente codice, nell'ambito di una verifica preliminare all'inizio del trattamento, effettuata anche in relazione a determinate categorie di titolari o di trattamenti, anche a seguito di un interpello del titolare".

L'**art. 20** recante "Principi applicabili al trattamento di dati sensibili." prevede:

"1. Il trattamento dei dati sensibili da parte di soggetti pubblici è consentito solo se autorizzato da espressa disposizione di legge nella quale sono specificati i tipi di dati che possono essere trattati e di operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite. 2. Nei casi in cui una disposizione di legge specifica la finalità di rilevante interesse pubblico, ma non i tipi di dati sensibili e di operazioni eseguibili, il trattamento è consentito solo in riferimento ai tipi di dati e di operazioni identificati e resi pubblici a cura dei soggetti che ne effettuano il trattamento, in relazione alle specifiche finalità perseguite nei singoli casi e nel rispetto dei principi di cui all'articolo 22, con atto di natura regolamentare adottato in conformità al parere espresso dal Garante ai sensi dell'articolo 154, comma 1, lettera g), anche su schemi tipo. 3. Se il trattamento non è previsto espressamente da una disposizione di legge i soggetti pubblici possono richiedere al Garante l'individuazione delle attività, tra quelle demandate ai medesimi soggetti dalla legge, che perseguono finalità di rilevante interesse pubblico e per le quali è conseguentemente autorizzato, ai sensi dell'articolo 26, comma 2, il trattamento dei dati sensibili. Il trattamento è consentito solo se il soggetto pubblico provvede altresì a identificare e rendere pubblici i tipi di dati e di operazioni nei modi di cui al comma 2. 4. L'identificazione dei tipi di dati e di operazioni di cui ai commi 2 e 3 è aggiornata e integrata periodicamente".

L'**art. 21** recante "Principi applicabili al trattamento di dati giudiziari." prevede:

"1. Il trattamento di dati giudiziari da parte di soggetti pubblici è consentito solo se autorizzato da espressa disposizione di legge o provvedimento del Garante che specifichino le finalità di rilevante interesse pubblico del trattamento, i tipi di dati trattati e di operazioni eseguibili.2. Le disposizioni di cui all'articolo 20, commi 2 e 4, si applicano anche al trattamento dei dati giudiziari".

L'**art. 22, commi 8 e 10, 11,** recante "Principi applicabili al trattamento di dati sensibili e giudiziari" prevede:

"8. I dati idonei a rivelare lo stato di salute non possono essere diffusi.10. I dati sensibili e giudiziari non possono essere trattati nell'àmbito di test psico-attitudinali volti a definire il profilo o la personalità dell'interessato. Le operazioni di raffronto tra dati sensibili e giudiziari, nonché i trattamenti di dati sensibili e giudiziari ai sensi dell'articolo 14, sono effettuati solo previa annotazione scritta dei motivi. 11. In ogni caso, le operazioni e i trattamenti di cui al comma 10, se effettuati utilizzando banche di dati di diversi titolari, nonché la diffusione dei dati sensibili e giudiziari, sono ammessi solo se previsti da espressa disposizione di legge".

L'**art. 25** recante "Divieti di comunicazione e diffusione" prevede:

"1. La comunicazione e la diffusione sono vietate, oltre che in caso di divieto disposto dal Garante o dall'autorità giudiziaria:

a) in riferimento a dati personali dei quali è stata ordinata la cancellazione, ovvero quando è decorso il periodo di tempo indicato nell'articolo 11, comma 1, lettera e); b) per finalità diverse da quelle indicate nella notificazione del trattamento, ove prescritta. 2. È fatta salva la comunicazione o diffusione di dati richieste, in conformità alla legge, da forze di polizia, dall'autorità giudiziaria, da organismi di informazione e sicurezza o da altri soggetti pubblici ai sensi dell'articolo 58, comma 2, per finalità di difesa o di sicurezza dello Stato o di prevenzione, accertamento o repressione di reati".

L'**art. 26** recante "Garanzie per i dati sensibili" prevede:

"1. I dati sensibili possono essere oggetto di trattamento solo con il consenso scritto dell'interessato e previa autorizzazione del Garante, nell'osservanza dei presupposti e dei limiti stabiliti dal presente codice, nonché dalla legge e dai regolamenti. 2. Il Garante comunica la decisione adottata sulla richiesta di autorizzazione entro quarantacinque giorni, decorsi i quali la mancata pronuncia equivale a rigetto. Con il provvedimento di autorizzazione, ovvero successivamente, anche sulla base di eventuali verifiche, il Garante può prescrivere misure e accorgimenti a garanzia dell'interessato, che il titolare del trattamento è tenuto ad adottare. 3. Il comma 1 non si applica al trattamento: a) dei dati relativi agli aderenti alle confessioni religiose e ai soggetti che con riferimento a finalità di natura esclusivamente religiosa hanno contatti regolari con le medesime confessioni, effettuato dai relativi organi, ovvero da enti civilmente riconosciuti, sempre che i dati non siano diffusi o comunicati fuori delle medesime confessioni. Queste ultime determinano idonee garanzie relativamente ai trattamenti effettuati, nel rispetto dei princìpi indicati al riguardo con autorizzazione del Garante; b) dei dati riguardanti l'adesione di associazioni od organizzazioni a carattere sindacale o di categoria ad altre associazioni, organizzazioni o confederazioni a carattere sindacale o di categoria. 4. I dati sensibili possono essere oggetto di trattamento anche senza consenso, previa autorizzazione del Garante: a) quando il trattamento è effettuato da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale, ivi compresi partiti e movimenti politici, per il perseguimento di scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto o dal contratto collettivo, relativamente ai dati personali degli aderenti o dei soggetti che in relazione a tali finalità hanno contatti regolari con l'associazione, ente od organismo, sempre che i dati non siano comunicati all'esterno o diffusi e l'ente, associazione od organismo determini idonee garanzie relativamente ai trattamenti effettuati, prevedendo espressamente le modalità di utilizzo dei dati con determinazione resa nota agli interessati all'atto dell'informativa ai sensi dell'articolo 13; b) quando il trattamento è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo. Se la medesima finalità riguarda l'interessato e quest'ultimo non può prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità di intendere o di volere, il consenso è manifestato da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato. Si applica la disposizione di cui all'articolo 82, comma 2; c) quando il trattamento è necessario ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere in sede giudiziaria un diritto, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento. Se i dati sono idonei a rivelare lo stato di salute e la vita sessuale, il diritto deve essere di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile; d) quando è necessario per adempiere a specifici obblighi o compiti previsti dalla legge, da un regolamento o dalla normativa comunitaria per la gestione del rapporto di lavoro, anche in materia di igiene e sicurezza del lavoro e della popolazione e di previdenza e assistenza, nei limiti previsti dall'autorizzazione e ferme restando le disposizioni del codice di deontologia e di buona condotta di cui all'articolo 111. 5. I dati idonei a rivelare lo stato di salute non possono essere diffusi".

L'**art. 27** recante "Garanzie per i dati giudiziari" prevede:

"1. Il trattamento di dati giudiziari da parte di privati o di enti pubblici economici è consentito soltanto se autorizzato da espressa disposizione di legge o provvedimento del Garante che specifichino le rilevanti finalità di interesse pubblico del trattamento, i tipi di dati trattati e di operazioni eseguibili".

L'**art. 45** recante "Trasferimenti vietati" prevede:

"1. Fuori dei casi di cui agli articoli 43 e 44, il trasferimento anche temporaneo fuori del territorio dello Stato, con qualsiasi forma o mezzo, di dati personali oggetto di trattamento, diretto verso un Paese non appartenente all'Unione europea, è vietato quando l'ordinamento del Paese di destinazione o di transito dei dati non assicura un livello di tutela delle persone adeguato. Sono valutate anche le modalità del trasferimento e dei trattamenti previsti, le relative finalità, la natura dei dati e le misure di sicurezza".

Segue Tab. 3

ILLECITI PENALI[11]	
Illecito	*Sanzioni penali*
169. Misure di sicurezza Chiunque, essendovi tenuto, omette di adottare le misure minime previste dall'articolo 33.	▪ Arresto sino a due anni o con l'ammenda da diecimila euro a cinquantamila euro.
All'autore del reato, all'atto dell'accertamento o, nei casi complessi, anche con successivo atto del Garante.	▪ E' impartita una prescrizione fissando un termine per la regolarizzazione non eccedente il periodo di tempo tecnicamente necessario, prorogabile in caso di particolare complessità o per l'oggettiva difficoltà dell'adempimento e comunque non superiore a sei mesi. Nei sessanta giorni successivi allo scadere del termine, se risulta l'adempimento alla prescrizione, l'autore del reato è ammesso dal Garante a pagare una somma pari al quarto del massimo dell'ammenda stabilita per la contravvenzione. L'adempimento e il pagamento estinguono il reato.
170. Inosservanza di provvedimenti del Garante Chiunque, essendovi tenuto, non osserva il provvedimento adottato dal Garante ai sensi degli articoli 26, comma 2, 90, 150, commi 1 e 2, e 143, comma 1, lettera c).	▪ Reclusione da tre mesi a due anni.
171. Altre fattispecie. La violazione delle disposizioni di cui agli articoli 113, comma 1, e 114.	▪ Sanzioni di cui all'articolo 38 della legge 20 maggio 1970, n. 300

[11] **Sanzioni penali** – **Illecito Pena** - ***169 – Misure di sicurezza*** – Chiunque essendovi tenuto, omette di adottare le misure minime previste dall'art. 33 del "Codice". All'autore del reato all'atto dell'accertamento o, nei casi più complessi, con atto successivo del Garante: arresto sino a due anni o con l'ammenda da diecimila euro a cinquantamila euro. E' impartita una prescrizione fissando un termine per la regolarizzazione non eccedente il periodo di tempo tecnicamente necessario, prorogabile in caso di particolare complessità o per l'oggettiva difficoltà dell'adempimento e comunque non superiore a sei mesi.
Nei sessanta giorni successivi allo scadere del termine, se risulta l'adempimento alla prescrizione, l'autore del reato è ammesso dal Garante a pagare una somma pari al quarto del massimo dell'ammenda stabilita per la contravvenzione. L'adempimento e il pagamento estinguono il reato. ***170 – Inosservanza dei provvedimenti del gar****ante* - Chiunque, essendovi tenuto, non osserva il provvedimento adottato dal Garante ai sensi degli articoli 26, comma 2, 90, 150, commi 1 e 2, e 143, comma 1, lettera c), è punito con la reclusione da tre mesi a due anni. ***Art. 171 - Altre fattispecie*** - La violazione delle disposizioni di cui agli articoli 113, comma 1, e 114 è punita con le sanzioni di cui all'articolo 38 della legge 20 maggio 1970, n. 300.
Art. 172 - Pene accessorie - La condanna per uno dei delitti previsti dal presente codice importa la pubblicazione della sentenza.

CAPITOLO II

REGOLE SPECIFICHE PER ARS

CAPITOLO II
REGOLE SPECIFICHE PER ARS

2.1 Il Codice ed i riflessi sull'attività dell'ARS

2.1.1 Codici di deontologia e di buona condotta

L'Agenzia, in quanto ente pubblico soggiace alla disciplina del Codice cui si aggiunge il rispetto dei codici di deontologia e buona condotta come fonti di norme flessibili e agevolmente modificabili.
Il rispetto delle disposizioni dei codici costituisce condizione essenziale per la liceità e correttezza del trattamento di dati personali. Ad ARS si applica il Provvedimento 16 giugno 2004, n. 2 "*Codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e scientifici*" (pubblicato sulla G.U. n. 190 del 14 agosto 2004).
I Codici hanno lo scopo di assicurare l'equilibrio tra il diritto alla privacy e la necessità della ricerca scientifica e le ragioni che ne sono alla base: il principio della libertà della ricerca costituzionalmente garantito e le esigenze del relativo sviluppo per migliorare le condizioni della società. Inoltre i Codici completano il quadro delle regole del Codice Privacy, secondo un ragionevole principio di parsimonia, in base al quale deono essere utilizzati i dati anonimi quando siano sufficienti per gli scopi di ricerca.
Nei Codici sono individuati fra l'altro:

- ✓ i presupposti ed i procedimenti per documentare che i trattamenti siano svolti per idonei ed effettivi scopo statistici e di ricerca scientifica;
- ✓ le regole di correttezza da osservare nella raccolta dei dati;
- ✓ le misure di sicurezza da adottare per favorire il rispetto dei principi di pertinenza e non eccedenza dei dati e delle misure di sicurezza di cui all'art. 33 del Codice privacy.

Gli incaricati sono tenuti al rispetto delle disposizioni contenute nel Codice sopra citato.

2.1.2 La veste formale in cui agisce ARS

Gli impegni di ARS in materia di privacy assumono diversa natura in dipendenza della veste formale con cui agisce ARS o più precisamente in relazione alle finalità del trattamento eseguito, sia in riferimento all'attività delle strutture scientifiche, sia in relazione alle attività della struttura amministrativa. Per quanto sopra precede le finalità del trattamento e, quindi, la veste in cui opera l'Agenzia può essere riassunta in tre tipologie:

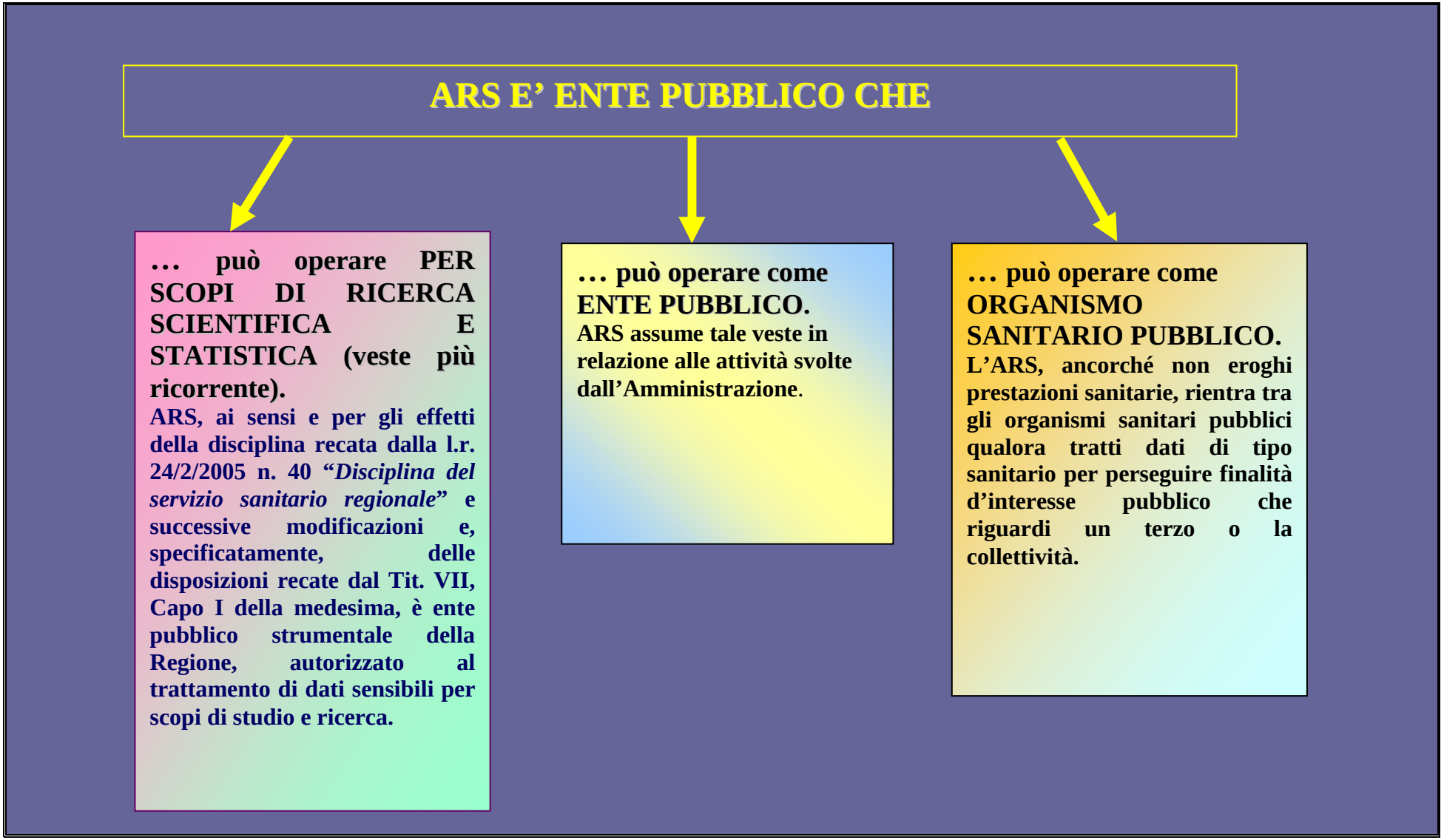
- ***Ente Pubblico che opera il trattamento di dati sensibili per scopi statistici o scientifici*** **(Strutture scientifiche)*;***

- *Ente Pubblico che opera il trattamento di dati sensibili in qualità di organismo sanitario pubblico per perseguire finalità di tutela della salute di un terzo o della collettività* (Strutture scientifiche);

- *Ente Pubblico che opera trattamento di dati sensibili o giudiziari per l'esercizio di attività amministrativa* (Struttura amministrativa).

La ***Tav. 3.*** che segue riassume le varie possibilità di operare di ARS

Tav. 3 - Le varie possibilità di operare di ARS



2.1.2.1. Trattamento dati sensibili per scopi statistici o scientifici

La tipologia dell'attività scientifica svolta dall'Agenzia rientra a pieno titolo, o forse sarebbe più opportuno dire *naturaliter,* cioè per sua vocazione naturale, nell'ambito della disciplina del trattamento per scopi scientifici contenuta al Capo III, agli articoli 104 e seguenti del "Codice".
Le disposizioni contenute in questo paragrafo in generale sono tese a garantire il corretto utilizzo di dati raccolti inizialmente per altri scopi, si pensi allo scopo sanitario, e dunque tese a garantire il corretto utilizzo ed il rispetto, nel caso di specie, della finalità scientifica.
Da qui la previsione del rispetto di codici di deontologia e di buona condotta (articolo 106)[12] di cui il Garante è promotore, nei quali è prevista tutta una dettagliata serie di disposizioni atte a garantire la correttezza del trattamento dei dati.
Ai fini della presente esposizione, rilevano:

- il combinato disposto degli articoli 20, comma 1, e 26, comma 3, secondo cui il trattamento dei dati sensibili è consentito ai soggetti pubblici e, quindi, **non è necessario richiedere l'autorizzazione al Garante,** solo se autorizzati da espressa disposizione di legge nella quale sono specificati i tipi di dati che possono essere trattati, le operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite. E' appunto il caso dell'Agenzia, ove operi per scopi statistici o scientifici in quanto a ciò autorizzata dalla legge istitutiva, con la quale si precisano le tipologie dei dati e le operazioni eseguibili[13];
- l'articolo 20, comma 2, secondo cui **vi è obbligo di adottare un atto di natura regolamentare** per il trattamento dei dati sensibili qualora questi non sia previsti dalla legge istitutiva[14];
- gli articoli 37, comma 1, lett. b) e 38, **che impongono l'obbligo di notificazione al Garante[15] prima di ogni trattamento ed una sola volta a prescindere dal numero delle operazioni e dalla durata del trattamento che può riguardare uno o più trattamenti con finalità correlate;**
- l'articolo 34, comma 1, lett. g) e All. B, in relazione al quale tutti i soggetti e, quindi, anche gli enti pubblici, erano obbligati entro il 30 dicembre 2004, ad adottare il Documento Programmatico sulla Sicurezza (DPS)[16], così come disciplinato dal decreto legge varato dal Governo il 22 giugno 2004. A regime, lo stesso deve essere aggiornato entro il 31 marzo di ogni anno in relazione all'evoluzione tecnica e all'esperienza maturata nel settore, secondo le decisioni adottate con Decreto del Ministro di grazia e giustizia assunte di concerto con il Ministro per le innovazioni tecnologiche. Dell'adozione e aggiornamento del DPS deve essere data notizia nella relazione di accompagnamento al bilancio d'esercizio dell'Ente.

---

[12] **Il Codice di deontologia per il trattamento dei dati sensibili per scopi statistici e scientifici è stato pubblicato sulla G.U. n. 190 del 14 agosto 2004.**
[13] **Sul tema si veda specificatamente il successivo paragr. 2.2.2.**
[14] **Sul tema si veda specificatamente il successivo paragr. 2.3.1.**
[15] **Sul tema si veda specificatamente il successivo paragr. 2.2.3**
[16] **Sul tema si veda specificatamente il successivo paragr. 2.3.2**

- l'articolo 39, comma 1, lett. b), **per il quale sussiste l'obbligo di comunicare[17] preventivamente al Garante il trattamento di dati idonei a rilevare lo stato di salute previsto da programmi di ricerca biomedica o sanitaria di cui all'art. 12/*bis* del d.lgs. 502/92 e ss.mm.;**
- gli articoli 109 e 110 che, espressamente, si occupano di dati sanitari. In particolare l'articolo 110 in tema di ricerca medica, biomedica ed epidemiologica prevede che "**Il consenso dell'interessato[18] per il trattamento dei dati idonei a rivelare lo stato di salute, finalizzato a scopi di ricerca scientifica in campo medico, biomedico o epidemiologico, non è necessario quando la ricerca è prevista da un'espressa disposizione di legge** che prevede specificamente il trattamento, ovvero rientra in un programma di ricerca biomedica o sanitaria previsto ai sensi dell'articolo 12-*bis* del decreto legislativo 30 dicembre 1992, n. 502 e successive modificazioni, e per il quale sono decorsi quarantacinque giorni dalla comunicazione al Garante ai sensi dell'articolo 39".

2.1.2.2 Trattamento dati sensibili in qualità di organismo sanitario pubblico per perseguire finalità di tutela della salute di un terzo o della collettività

Il "Codice"dedica un'ampia trattazione con riguardo ai dati in ambito sanitario. Dalle disposizioni in esso contenute, tuttavia, emerge una prima considerazione di ordine generale che attiene al dato che le disposizioni riguardano prevalentemente i soggetti sanitari (medici) e le strutture pubbliche o private che erogano direttamente prestazioni di natura sanitaria.
Alla luce di tale considerazione generale, dunque, è prioritario verificare se l'Agenzia possa collocarsi dal punto di vista giuridico e normativo nell'ambito "degli organismi sanitari pubblici" che, ai sensi degli articoli 76 e ss. del "Codice", sono destinatari della disciplina sul trattamento dei dati personali in ambito sanitario.
Tale verifica si ritiene, oltretutto, importante perché l'applicazione delle disposizioni in esame comporterebbe la necessità per l'Agenzia di acquisire la richiesta di autorizzazione al trattamento, da inoltrare al Garante ai sensi dell'articolo 76 del Codice privacy, qualora il trattamento riguardi dati e operazioni indispensabili per perseguire una finalità di tutela della salute di un terzo o della collettività. Nel successivo paragrafo che affronta i tempi connessi alla "autorizzazione al trattamento, da inoltrare al Garante viene dato ampio conto degli obblighi da adempiere.
Occorre precisare che l'analisi che segue affronta aspetti squisitamente giuridici e normativi che possono costituire il supporto alle decisione da assumere, in quanto la collocazione dell'Agenzia tra gli organismi sanitari pubblici ai quali fa riferimento il decreto probabilmente non può prescindere dalla valutazione diretta della finalità del trattamento.
Certamente l'Agenzia non è struttura che direttamente eroga prestazioni sanitarie. Tuttavia la sua qualificazione di organismo sanitario pubblico si ritiene non possa escludersi a priori ma al contrario possa affermarsi sulla scorta delle considerazioni che seguono.
Ai sensi dell'articolo 76 del "Codice", infatti, sono organismi sanitari pubblici, quelli che "anche nell'ambito di un'attività di rilevante interesse pubblico ai sensi

[17] **Sul tema si veda specificatamente il successivo paragr. 2.2.4**
[18] **Sul tema si veda specificatamente il successivo paragr. 2.3.3**

dell'articolo 85 dello stesso "Codice", trattano i dati personali idonei a rivelare lo stato di salute (….) " *per perseguire la finalità di tutela della salute di un terzo o della collettività".*
Ai sensi dell'articolo 85 (rubricato "*Compiti del Servizio sanitario nazionale*"), poi, si precisa che si considerano finalità di rilevante interesse pubblico le finalità che rientrano *"nei compiti del Servizio sanitario nazionale e degli altri organismi sanitari pubblici relative",* tra l'altro, si precisa l'attività di *"programmazione, gestione, controllo e valutazione dell'assistenza sanitaria".*
Si ritiene che l'analisi che precede fornisca elementi di per sé sufficienti a collocare l'Agenzia anche nell'ambito degli organismi sanitari pubblici ancorché non eroghi direttamente prestazioni sanitarie. Tuttavia a maggiore conferma di tale risultato si deve, poi, ricordare che l'enucleazione delle finalità che rientrano nei compiti del Servizio sanitario nazionale, potrebbe non risultare esaustiva perché oggetto di possibile integrazione con le ulteriori finalità di rilevante interesse pubblico individuate dalle regioni come accade, in particolare, nel caso in esame, dalla normativa della Regione Toscana.
Il passaggio ora delineato è strettamente connesso con la trattazione di ben più ampio respiro legata alla modifica del Titolo V della Costituzione ed, in particolare, alle rilevanti modifiche in ordine alla competenza legislativa delle regioni, anche in materia sanitaria che pur restando una competenza concorrente con la competenza statale, per il mutato quadro complessivo a livello costituzionale, può dirsi aver acquistato ben più ampia portata.
Non è questa la sede per simile approfondimento, tuttavia sia sufficiente notare che la Regione Toscana ha senza dubbio attribuito all'Agenzia un ruolo di rilevante interesse pubblico nell'ambito del Servizio sanitario regionale nel momento in cui, agli articoli 20, 82 e 82-*bis* della l.r. 40/2005 e ss.mm. attribuisce alla stessa importanti funzioni di supporto e consulenza al Consiglio, alla Giunta ed alle Aziende sanitarie, in materia, tra l'altro, di programmazione regionale, valutazione della sanità regionale, valutazione della programmazione.
Alla luce delle considerazioni svolte, ne discende come conseguenza la possibile applicazione del disposto dell'articolo 76, comma 1, lett. b), già in precedenza citato, secondo il quale *"Gli organismi sanitari pubblici, anche nell'ambito di un'attività di rilevante interesse pubblico ai sensi dell'articolo 85, trattano i dati personali idonei a rivelare lo stato di salute (..) anche senza il consenso dell'interessato e previa autorizzazione del Garante, se la finalità di (..) "*tutela della salute *" riguarda un terzo o la collettività".*

Le questioni poste possano essere di facile composizione ove si abbia cura di dichiarare esplicitamente la finalità del trattamento che, per l'ARS, può essere quasi sempre ricondotta agli scopi statistici o scientifici trattati al paragrafo 2.1.2 che precede, salvo che nell'affidamento di specifici progetti di studio e ricerca non sia dichiarato esplicitamente che la finalità di tutela della salute riguarda un terzo o la collettività.

Per la tipologia in esame si confermano le esenzioni, nonché tutti gli obblighi di adempimento già descritti al paragrafo 2.1.1 che precede, cui potrebbe aggiungersi:

- **l'obbligo di richiede l'autorizzazione al Garante** per il trattamento di dati sensibili. Tale autorizzazione è rilasciata, salvi i casi di particolare urgenza, sentito il Consiglio Superiore di Sanità.
  Per alleggerire gli oneri che incombono su coloro che trattano dati sensibili e giudiziari, il Garante ha tuttavia adottato una serie di autorizzazioni generali per particolari categorie di titolari o per specifici trattamenti di dati (art. 40 "Codice", tra questi specificatamente per gli organismi sanitari pubblici[19] **l'autorizzazione generale 2/2007 che di fatto esonera ARS da tale obbligo, qualora operi come organismo sanitario pubblico;**
- **l'informativa all'interessato è sempre dovuta ma si attua con modalità semplificata**[20]**;**

2.1.2.3. Trattamento dati sensibili e giudiziari per l'esercizio di attività amministrativa

Nell'esercizio dell'attività amministrativa l'ARS, in quanto ente pubblico, può trattare dati sensibili e giudiziari per finalità di rilevante interesse pubblico relativamente:

- all'insediamento, stato patrimoniale, assicurazioni, pagamento indennità, dimissioni, decadenza degli Organi;
- al reclutamento, costituzione del rapporto di lavoro e gestione del personale dipendente e a contratto;
- all'attività contrattuale, con specifico riferimento alla richiesta delle offerte, aggiudicazione e stipula di contratti;
- al contenzioso stragiudiziale**;**
- al contenzioso giudiziale.

Per la tipologia in esame, quando ARS opera nella veste di soggetto pubblico per l'esercizio di attività amministrative, si confermano le esenzioni, nonché tutti gli obblighi di adempimento già descritti al paragrafo 2.1.1 che precede, per ciò che concerne la notificazione, l'adozione di un atto di natura regolamentare e del DPS, cui si aggiunge:

- **l'obbligo di comunicare previamente al Garante** (art. 39, comma 1, lett. a) del Codice) la comunicazione di dati personali (sensibili o giudiziari) da parte di un soggetto pubblico ad altro soggetto pubblico **non prevista da una norma di legge o di regolamento**, effettuata in qualunque forma anche mediante convenzione.
  Al riguardo si precisa che si rende assolutamente necessario per gli incaricati della struttura amministrativa analizzare di volta in volta, con il conforto del Gruppo privacy, la tipologia del dato da trasmettere, al fine di verificare se la trasmissione ad altro Ente sia o meno disciplinata da legge o regolamento (si veda anche al riguardo quanto specificatamente contenuto nel Cap. III riferito alle prescrizioni specifiche impartite per la Direzione);

Oltre agli obblighi anzidetti, le disposizioni del Codice introdurrebbe anche:

---

[19] **Si veda al riguardo il successivo paragr. 2.2.2**
[20] **Si veda al riguardo il successivo paragr. 2.3.3.1.**

- **l'obbligo di richiedere l'autorizzazione al Garante** per il trattamento di dati sensibili e giudiziari **non previsti da norma di legge o regolamento.**
  Per alleggerire gli oneri che incombono su coloro che trattano dati sensibili e giudiziari, il Garante ha tuttavia adottato una serie di autorizzazioni generali per particolari categorie di titolari o per specifici trattamenti di dati (art. 40 "Codice", tra queste rilevano ai fini della presente disamina le autorizzazione generali 1, 2 e 7 del 2007, che di fatto esonerano ARS da tale obbligo[21].

I paragrafi che seguono affrontano nello specifico tutti gli adempimenti sinteticamente decritti nel presente paragrafo suddivisi tra:

- **Adempimenti a rilevanza esterna da assolvere nei confronti del Garante** (paragr. 2.2);
- **Adempimenti rilevanti** (paragr. 2.3).

In ultimo gli stessi adempimenti sono ricondotti e sintetizzati in apposite tabelle (paragr. 2.4).

[21] Si veda al riguardo specificatamente il paragrafo 2.2.2.

2.2 Adempimenti a rilevanza esterna da assolvere nei confronti del Garante

2.2.1 rapporti con l'Autorità Garante

Ogni rapporto formale o adempimento di legge nei confronti o verso l'Autorità Garante per gli aspetti tecnico-operativi connessi all'attuazione del Codice: richieste di chiarimenti, richieste di pareri formali, richieste di autorizzazioni, comunicazioni, notificazioni etc., compete al Titolare il quale vi provvede avvalendosi del Gruppo Privacy che opera a supporto delle strutture organizzative di ARS al fine di evitare frammentazioni.
Il paragrafo ripercorre tutti gli adempimenti verso il Garante in relazione ai quali gli incaricati sono tenuti a collaborare con il Gruppo Privacy affinché gli stessi possano essere assolti dal Titolare di ARS; il paragrafo illustra le finalità che il Codice si propone e la pratica attuazione degli obblighi che ne derivano.

2.2.2 Autorizzazione

In via generale il "Codice" dispone che i dati personali sensibili e/o giudiziari possono essere trattati solo previa Autorizzazione del Garante (artt. 26 e 27 del Codice).
Tale autorizzazione riguarda il trattamento dei dati sensibili e giudiziari, da parte di soggetti privati, ai sensi dell'articolo 26 del codice della privacy, e da parte dei soggetti pubblici, secondo quanto previsto dal combinato disposto degli articoli 20, comma 1, e 26, comma 3, **ove il trattamento non sia previsto espressamente da una disposizione di legge.**
Ai sensi dell'art. 41, comma 3, del d.lgs. n. 196/2003 l'eventuale richiesta di autorizzazione è formulata utilizzando esclusivamente il modello predisposto e reso disponibile dal Garante e trasmessa a questo ultimo per via telematica, osservando le modalità di sottoscrizione e conferma del ricevimento di cui all'articolo 38, comma 2. La medesima richiesta e l'autorizzazione possono essere trasmesse anche mediante telefax o lettera raccomandata.

Tale previsione generale non è riconducibile ad ARS posto che l'Agenzia è autorizzata dalla legge istitutiva al trattamento di dati sensibili.

Il "Codice", introduce, viceversa alcune specifiche garanzie di tutela relativamente:

- **al trattamento di dati sensibili effettuati dagli organismi sanitari pubblici (Art. 76).** L'ARS sarebbe, quindi, sottoposta all'obbligo di chiedere l'autorizzazione nell'ipotesi in cui la stessa operasse come "organismo sanitario pubblico". In questo caso, infatti, il trattamento dei dati personali idonei a rivelare lo stato di salute sarebbe possibile solo previa autorizzazione del Garante, autorizzazione rilasciata, salvi i casi di particolare urgenza, sentito il Consiglio superiore di sanità;
- **al trattamento di dati sensibili e giudiziari** da parte di privati, di enti pubblici economici e **di soggetti pubblici, non previsto da norma di legge o regolamento**. L'ARS sarebbe, quindi, sottoposta all'obbligo di chiedere la preventiva autorizzazione nell'ipotesi in cui la stessa operasse il trattamento di dati

sensibili o giudiziari in qualità di Ente pubblico per attività afferenti alla struttura amministrativa, **non previste da legge o regolamento**.

Per alleggerire gli oneri che incombono su coloro che trattano dati sensibili e giudiziari, il Garante ha, tuttavia, adottato una serie di autorizzazioni generali per particolari categorie di titolari o per specifici trattamenti di dati (art. 40).

Nella Relazione al Parlamento 1997, il Garante si è espresso in materia di autorizzazioni generali disponendo che:

a) "le autorizzazioni per categorie o collettive permettono all'organo di garanzia di svolgere la propria azione di tutela con organicità, procedendo attraverso ampie aggregazioni di attività omogenee e rivolgendosi non più in maniera frammentaria e parcellizzata a singoli soggetti, ma ad intere categorie. La generalità dell'approccio valorizza lo strumento autorizzativo, che da provvedimento di disciplina di specifiche situazioni diviene una fonte di regolamentazione più ampia di interessi di rango quasi normativo;
b) tale metodo conferisce alla formula autorizzatoria la possibilità di individuazione di momenti unitari, che rendono agevole e snella la salvaguardia di principi inderogabili connessi ai dati sensibili;
c) l'autorizzazione collettiva non soltanto si ispira ai principi di snellimento dell'azione amministrativa, ma comporta una notevole semplificazione degli adempimenti spettanti ai soggetti preposti al trattamento e incide positivamente sui loro profili economici, implicando un risparmio nei costi di gestione."

Le autorizzazioni generali[22], nello specifico, sono:

- **Autorizzazione n. 1/2007** al trattamento dei dati sensibili nei rapporti di lavoro.
- **Autorizzazione n. 2/2007** al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale.
- **Autorizzazione n. 3/2007** al trattamento dei dati sensibili da parte degli organismi di tipo associativo e delle fondazioni.
- **Autorizzazione n. 4/2007** al trattamento dei dati sensibili da parte dei liberi professionisti.
- **Autorizzazione n. 5/2007** al trattamento dei dati sensibili da parte di diverse categorie di titolari.
- **Autorizzazione n. 6/2007** al trattamento dei dati sensibili da parte degli investigatori privati.
- **Autorizzazione n. 7/2007** al trattamento dei dati a carattere giudiziario da parte di privati, di enti pubblici economici e di soggetti pubblici.

I testi sono disponibili in internet all'indirizzo www.garanteprivacy.it.

Ai fini delle presenti prescrizioni, pertanto, non sussiste al momento alcun obbligo per ARS, qualunque sia la veste in cui la stessa opera, di richiedere preventivamente l'autorizzazione del Garante, sia per il trattamento di dati sensibili sia per il trattamento di quelli giudiziari, alla luce delle seguenti motivazioni:

- **ARS è sicuramente autorizzata dalla legge istitutiva al trattamento di dati sensibili per l'esercizio delle attività a carattere scientifico, nonché per il**

[22] Il Garante, nel dicembre 2005, ha rilasciato le nuove autorizzazioni al trattamento dei dati sensibili e giudiziari, successivamente rinnovate.
Le nuove autorizzazioni non recano significative modifiche rispetto a quelle in corso di efficacia, alle quali sono state apportate solo alcune circoscritte integrazioni relative a modifiche normative intervenute nei settori considerati, in particolare per quanto riguarda i rapporti di lavoro.

trattamento di dati sensibili e giudiziari afferenti ad attività amministrative espressamente autorizzate sia dalla legge istitutiva sia da specifiche disposizioni normative;

- **ARS non è soggetto all'obbligo di richiedere la preventiva autorizzazione al Garante per effetto delle autorizzazioni generali sopra richiamate e, tra esse, specificatamente:**
  - ✓ **Autorizzazione n. 1/2007 al** trattamento dei dati sensibili nei rapporti di lavoro;
  - ✓ **Autorizzazione n. 2/2007** al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale;
  - ✓ **Autorizzazione n. 7/2007** al trattamento dei dati a carattere giudiziario da parte di privati, di enti pubblici economici e di soggetti pubblici.

Attenzione tuttavia va posta in ordine alle successive decisioni del Garante che, per pura ipotesi, potrebbero eliminare le autorizzazioni generali concesse. Il Gruppo Privacy di cui al paragrafo 2.5.1. ha il compito di segnalare le novità che dovessero intervenire.

2.2.3 Notificazione

La notificazione è la dichiarazione con la quale un soggetto pubblico (o privato) rende nota al Garante per la protezione dei dati personali l'esistenza di un'attività di raccolta e utilizzazione dei dati personali, **svolta quale autonomo Titolare del trattamento** (art. 37 Codice).

Mentre la normativa previgente stabiliva l'obbligo di notificazione in capo a tutti i soggetti non esplicitamente esentati, il T.U. rovescia l'impostazione e indica solo i casi in cui sussiste l'obbligo in oggetto.

Quando è obbligatoria la notifica per l'ARS?

Per ARS sussiste l'obbligo di notificazione relativamente ai:

a) dati idonei a rivelare lo stato di salute e la vita sessuale, trattati a fini di procreazione assistita, indagini epidemiologiche, rilevazione di malattie mentali, infettive e diffusive, sieropositività, trapianto di organi e tessuti e monitoraggio della spesa sanitaria;
b) dati idonei a rivelare la vita sessuale o la sfera psichica;
c) dati trattati con l'ausilio di strumenti elettronici volti a definire il profilo o la personalità dell'interessato, ovvero ad analizzare abitudini;
d) dati sensibili registrati in banche di dati a fini di selezione del personale per conto terzi;
e) dati registrati in apposite banche di dati gestite con strumenti elettronici e relative al rischio sulla solvibilità economica, alla situazione patrimoniale.

Con parere del 23 aprile 2004 il Garante ha forniti chiarimenti sui provvedimenti da notificare.

Il Garante si è riservato, tuttavia, la facoltà di individuare, con proprio provvedimento, altri trattamenti suscettibili di creare rischi specifici per i quali potrebbe essere richiesto l'obbligo di notificazione. I casi previsti in particolare sono riconducibili ai:

- **trattamenti** di dati diversi da quelli sensibili e giudiziari **suscettibili di recare pregiudizio ai diritti, alle libertà ed alla dignità dell'interessato**:
  - ✓ in ragione delle relative modalità di trattamento;
  - ✓ a causa della natura dei dati;
- **trattamenti individuati dal Garante**[23]
  - ✓ con proprio provvedimento adottato anche sulla base di una verifica preliminare, prescrivendo le misure e gli accorgimenti necessari:
    - anche a seguito di un interpello del titolare;
    - anche per categorie di titolari o trattamenti.

Il Codice demanda, altresì, al Garante il compito di individuare, tra i trattamenti di dati da notificare al medesimo specificati all'art. 37, quelli da sottrarre all'obbligo di notificazione, purché non suscettibili di recare pregiudizio ai diritti e alle libertà dell'interessato in ragione delle modalità di trattamento o della natura dei dati (art. 37, comma 1).

Con delib. Garante protez. dati pers. 31 marzo 2004, n. 1 *(Gazz. Uff. 6 aprile 2004, n. 81)* sono stati individuati i casi **da sottrarre all'obbligo di notificazione al Garante.**
In sede di prima applicazione del Codice il Garante ha, infatti, rilevato che taluni trattamenti sono effettuati con modalità che permettono, allo stato, di essere sottratti all'obbligo di notificazione, ferma restando l'osservanza degli ulteriori principi ed obblighi previsti dal Codice in materia di protezione dei dati personali.
In particolare assumono rilievo per ARS:

- ✓ ***con riferimento ai casi di cui al comma 1, lett. c), dell'art. 37 del Codice,*** i trattamenti di dati idonei a rivelare la sfera psichica di lavoratori effettuati da associazioni, enti od organismi a carattere sindacale per adempiere esclusivamente a specifici obblighi o compiti previsti dalla normativa in materia di rapporto di lavoro o di previdenza, anche in tema di diritto al lavoro dei disabili;
- ✓ ***con riferimento ai casi di cui al comma 1, lett. d) della medesima disposizione,*** i trattamenti di dati personali che non siano fondati unicamente su un trattamento automatizzato volto a definire profili professionali, effettuati per esclusive finalità di occupazione o di gestione del rapporto di lavoro, fuori dei casi di cui alla lettera e) del medesimo art. 37, comma 1;
- ✓ ***con riferimento ai casi di cui al comma 1, lett. e) della medesima disposizione,*** i trattamenti di dati sensibili effettuati da soggetti pubblici per adempiere esclusivamente a specifici obblighi o compiti previsti dalla normativa in materia di occupazione e mercato del lavoro;
- ✓ ***con riferimento ai casi di cui al comma 1, lett. f), della medesima disposizione, i trattamenti di dati personali:***
  - effettuati da soggetti pubblici per la tenuta di pubblici registri o elenchi conoscibili da chiunque;
  - registrati in banche di dati utilizzate in rapporti con l'interessato di fornitura di beni, prestazioni o servizi, o per adempimenti contabili o fiscali, anche in

[23] Il Garante allo stato di elaborazione delle presenti prescrizioni non ha assunto al riguardo alcun provvedimento.

caso di inadempimenti contrattuali, azioni di recupero del credito e contenzioso con l'interessato;
- registrati in banche di dati utilizzate da soggetti pubblici o privati per adempiere esclusivamente ad obblighi normativi in materia di rapporto di lavoro, previdenza o assistenza;
- relativi a immagini o suoni conservati temporaneamente per esclusive finalità di sicurezza o di tutela delle persone o del patrimonio.

La notificazione del trattamento è presentata al Garante prima dell'inizio del trattamento ed una sola volta, a prescindere dal numero delle operazioni e della durata del trattamento da effettuare e può anche riguardare uno o più trattamenti con finalità correlate.
La notificazione consiste in un modello contenente tutta una serie di dati, tra cui quelli relativi al trattamenti effettuati, alle modalità ed alle finalità del trattamento, alle misure di sicurezza adottate.
Una nuova notificazione è richiesta solo prima della cessazione del trattamento e prima del mutamento di taluno degli elementi del trattamento da indicare nella notificazione.

In data 16/07/2004, ARS ha provveduto a trasmettere la notificazione per via telematica, ***(Allegato sub lettera "A")*** utilizzando il modello predisposto dal Garante, disponibile sul sito web del Garante www.garanteprivacy.it ed osservando le sue prescrizioni.
Il modello telematico è stato sottoscritto con firma digitale e trasmesso mediante intermediario convenzionato.
Si ritiene opportuno sottolineare che è fondamentale, ai fini di una corretta applicazione delle prescrizione del Codice privacy, che la notificazione risulti sempre aggiornata, per non incorrere nelle sanzioni che il T.U. collega alla violazione delle disposizioni in materia.
Il rischio di mancato aggiornamento della notificazione è, tuttavia, pressoché inesistente, visto che il documento è stato elaborato, in conformità alle indicazioni dello stesso Garante, nel modo più generico possibile, per farvi includere tutti i trattamenti che ARS può gestire.
Per l'omessa o incompleta notificazione al Garante sono previste sanzioni pecuniarie da € 10.000 a € 60.000 e la sanzione amministrativa accessoria della pubblicazione dell'ordinanza-ingiunzione, per intero o per estratto, in uno o più giornali indicati nel provvedimento che la applica (artt. 37 e 163).

Il Gruppo Privacy provvederà a segnalare al Titolare le novità che dovessero intervenire ai fini dell'integrazione/modifica dei trattamenti indicati nella notificazione.

Al fine di non incorrere nelle sanzioni predette è necessario che si instauri una forte interazione tra gli operatori di ARS incaricati del trattamento e il Gruppo Privacy, nel senso che **gli stessi devono provvedere a segnalare tempestivamente al Gruppo ogni nuovo trattamento, i trattamenti variati o cessati, di cui ARS è titolare unico, per consentire al Gruppo medesimo di verificare se sia necessario o meno integrare/modificare l'elenco già notificato.**

2.2.4 Comunicazione al Garante (Art. 39)

Per ARS sussiste l'obbligo di comunicare preventivamente al Garante, tramite il titolare del trattamento, le circostanze sotto riportate:

- **trattamento di dati idonei a rivelare lo stato di salute previsto dal programma di ricerca biomedica e/o sanitaria** (regolata dall'art. 12-*bis* del d.lgs. 502/1992), relativamente all'attività delle strutture scientifiche;
- **comunicazione di dati personali (sensibili/giudiziari) ad altro soggetto pubblico non prevista da norma di legge o di regolamento**, effettuata in qualunque forma anche mediante convenzione.
  Tale obbligo è riconducibile solo ad attività di competenza della struttura amministrativa, posto che per i dati inerenti lo stato di salute o la vita sessuale di competenza delle strutture scientifiche, ARS è autorizzata al loro trasferimento dalla legge istitutiva. In tal caso, l'opportunità della comunicazione al Garante è valutata di volta in volta in ordine alla circostanza che la comunicazione dei dati di cui trattasi ad altro soggetto pubblico sia o meno prevista da legge o regolamento.

La comunicazione è inviata utilizzando il modello che dovrà essere predisposto dal Garante, **non ancora reso disponibile**[24].

Nelle ipotesi di cui sopra, occorre osservare il seguente iter procedurale:

- ✓ i trattamenti iniziano decorso il termine di 45 giorni dalla data di ricevimento della comunicazione, salvo una diversa determinazione del Garante, che può essere anche emessa *ex post*;
- ✓ la comunicazione avviene mediante un modello standard predisposto dal Garante;
- ✓ la comunicazione è trasmessa:
  - per via telematica (sottoscrizione digitale);
  - mediante telefax;
  - mediante lettera raccomandata.

2.3. Adempimenti rilevanti

2.3.1 Regolamento

L'art. 20 del "Codice", precisa che il trattamento dei dati sensibili da parte di soggetti pubblici è consentito solo se autorizzato da espressa disposizione di legge nella quale sono specificati i tipi di dati che possono essere trattati, le operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite. Nei casi in cui una disposizione di legge specifica la finalità di rilevante interesse pubblico, ma non i tipi di dati sensibili e di operazioni eseguibili, il trattamento è consentito solo in riferimento ai tipi di dati e di operazioni identificati e resi pubblici con atto di natura regolamentare adottato in conformità al parere espresso dal Garante.

Allo stato:

[24] In ordine alle circostanze menzionate, **attualmente ARS non ha ancora provveduto alla comunicazione al Garante vista la mancata predisposizione da parte di questo ultimo del modello standard.** Il Gruppo Privacy provvederà a segnalare l'avvenuta predisposizione del modello di cui trattasi.

Il 28 marzo 2006, la Conferenza delle Regioni e Province autonome ha approvato lo schema tipo di regolamento necessario per gli enti non espressamente autorizzati a livello legislativo al trattamento dei dati personali.

Il 18 Aprile 2006 l'Autorità Garante ha espresso il parere favorevole sullo schema tipo predisposto dalla Conferenza, ai sensi dell'articolo 20 del Codice privacy (d.lgs. 196/03).

La Regione Toscana, in applicazione della disciplina recata dal "Codice" e dalle sopra citate disposizioni, ha approvato la *legge regionale 3 aprile 2006, n. 13 (Trattamento dei dati sensibili e giudiziari da parte della Regione Toscana, aziende sanitarie, enti, aziende e agenzie regionali e soggetti pubblici nei confronti dei quali la Regione esercita poteri di indirizzo e di controllo).*
Per la Regione l'intervento normativo si è reso necessario per adempiere agli obblighi della disciplina recata dagli articoli 20, comma 1 e 21, comma 2, del "Codice" specificando che il trattamento dei dati sensibili e giudiziari da parte della Giunta regionale, delle aziende sanitari e agenzie regionali, è disciplinato con regolamento della Giunta regionale. E' fatta salva la competenza all'adozione dell'atto di natura regolamentare in capo al Consiglio regionale per i trattamenti di dati sensibili e giudiziari di sua competenza.
Il Garante, infatti, a fronte di una specifica richiesta avanzata dalla Conferenza dei Presidenti dell'Assemblea dei Consigli regionali e delle Province Autonome, ha ammesso, in linea di principio, la legittimità di tale soluzione, rinviando ai singoli Statuti regionali per la valutazione dell'esistenza di un distinto potere decisionale, anche in materia di potestà regolamentare.
Per quanto sopra espresso la Regione Toscana ha adottato il Regolamento per la disciplina dei trattamenti di dati personali sensibili e giudiziari, individuando nella Giunta e nel Consiglio regionale, ognuno per le rispettive competenze, due distinti Titolari di trattamento e attribuendo, contestualmente, ai medesimi Organi, la potestà regolamentare.
Il regolamento *de quo* si configura come regolamento attuativo di legge statale (Codice) e come tale non rientra in nessuna delle tipologie di regolamento previste dall'articolo 42 dello Statuto della nostra Regione, che si limita a disciplinare la fattispecie di "regolamento":

- ✓ regolamenti di attuazione delle leggi regionali;
- ✓ regolamenti delegati dallo Stato;
- ✓ regolamenti di attuazione degli atti e delle norme comunitarie.

Con decreto del Presidente della Regione Toscana del 16/05/2006 n. 18/r, pertanto, è stato approvato il regolamento per il trattamento di dati sensibili e giudiziari di cui sono titolari la Regione Toscana - Giunta regionale, le aziende sanitarie, gli enti e le agenzie regionali e gli altri enti per i quali la Regione esercita poteri d'indirizzo e di controllo.
Da tale regolamento sono esclusi i trattamenti già adeguatamente regolati a livello legislativo e regolamentare per ciò che concerne i tipi dei dati e le operazioni eseguibili.

Nel regolamento in parola l'ARS è parzialmente inclusa per ciò che concerne i tipi di dati che afferiscono all'attività di ricerca e studio degli Osservatori dell'Agenzia, in

quanto i medesimi erano già adeguatamente regolati dalla legge che disciplinava l'Ente, l.r. 8 marzo 2000. n. 22, poi confluita nella richiamata l.r. 40/2005 e ss.mm., con cui già venivano specificati i trattamenti e le operazioni eseguibili.

Alle motivazioni sopra esposte occorre aggiungere che detta previsione regolamentare risulta ampiamente superata per effetto della successiva entrata in vigore della l.r. 28/2006[25] con cui si è proceduto a definire una nuovo assetto istituzionale ed organizzativo dell'Agenzia.
Al fine di sgombrare il campo da ogni dubbio interpretativo, vale la pena sottolineare che la circostanza più volte sollevata in ordine all'impossibilità dell'ARS di trattare i dati sensibili in quanto non espressamente previsto dal regolamento regionale approvato con DPGR 16 maggio 2006, n. 18/R, deve necessariamente essere commisurata alle disposizioni recate dalla legge regionale 10 luglio 2006, n. 28 "*Modifiche alla legge regionale 24 febbraio 2005, n. 40 (Disciplina del servizio sanitario regionale). Nuova disciplina dell'Agenzia regionale di sanità.*"; **la stessa norma, infatti, per il principio di gerarchia delle fonti, è prevalente in quanto fonte di rango superiore ed intervenuta in via temporale successivamente all'approvazione del regolamento di cui trattasi.**

E' da concludersi che è fuori di dubbio che l'ARS possa trattare i dati sensibili per l'esercizio delle funzioni istituzionali per effetto del combinato disposto della disciplina recata dall'art. 20 del "Codice Privacy" e le disposizioni normative di cui agli articoli 82 e segg. della l.r. 40/2005 e ss.mm,.

In ultimo, vale al riguardo la pena di richiamare l'attenzione sulla circostanza che in sede di esame da parte del Governo della l.r. 10 luglio 2006, n. 28, perplessità furono sollevate dal Garante Privacy in ordine alle disposizioni che autorizzavano l'ARS al trattamento dei dati sensibili. La risposta del Governatore della Regione permise di superare i rilievi mossi sui seguenti punti in ordine ai quali sono state svolte le argomentazioni che seguono:

- ✓ si condivideva l'affermazione che la disciplina della protezione dei dati personali, è riconducibile alla conformazione dei diritti fondamentali della persona il cui livello di tutela "non può che essere uniforme a livello nazionale", anche in coerenza con atti internazionali quali la Convenzione di Strasburgo e che, quindi, quindi è esclusa la configurabilità, in materia di protezione dei dati personali di una competenza regionale, sussistendo invece la potestà legislativa esclusiva dello Stato, in base all'articolo 117, secondo comma lettera l), m) e r) della Costituzione;
- ✓ tale esclusione di competenza doveva, tuttavia, essere rilegata alla necessità di garantire i diritti fondamentali della persona e che i trattamenti, pertanto, devono essere effettuati in modo lecito e corretto, pertinente e non eccedente rispetto alle finalità di utilizzo e dovrà essere garantita la conservazione finalizzata all'identificazione dell'interessato per il periodo necessario al raggiungimento dello scopo di raccolta e trattamento;

[25] La L.R. 10 luglio 2006, n. 28 *"Modifiche alla legge regionale 24 febbraio 2005, n. 40 (Disciplina del servizio sanitario regionale) - Nuova disciplina dell'Agenzia regionale di sanità"* e ss.mm., ha apportato modifiche ed integrazioni alla l.r. 40/2005 e ss.mm., introducendo una novellata disciplina per l'Agenzia regionale di Sanità, già regolata dalla l.r. 8 marzo 2000, n. 22 e ss.mm.

- ✓ la l.r. 28/2006 della Regione Toscana non aveva quindi inteso invadere la sfera di competenza statale circa le "modalità del trattamento" che garantiscono il diritto alla dignità della persona, limitandosi, viceversa, a disciplinare l'organizzazione del proprio servizio sanitario regionale, all'interno del quale ha inteso confermare, con novellata disciplina, un Ente strumentale della Regione con compiti di supporto tecnico-scientifico alla Giunta ed al Consiglio regionale ai fini della conoscenza dei bisogni di salute dei cittadini residente nel proprio territorio. L'Ente, infatti, è chiamato a svolgere attività di studio e ricerca in materia di epidemiologia e verifica della qualità dei servizi sanitari a supporto dei processi di programmazione regionale;
- ✓ l'analisi del nuovo assetto complessivo delle competenze legislative statali e regionali conseguente all'entrata in vigore della legge Costituzionale 18 ottobre 2001, n. 3, impostato esclusivamente sul criterio dell'esclusività, che si riflette anche sul piano della competenza concorrente, conduce ad affermare che la riforma del Titolo V della Costituzione, introdotta con legge Costituzionale 3/2001 inserisce tra le materie di legislazione concorrente anche quella relative alla tutela della salute.
- ✓ nelle materie di legislazione concorrente, spetta alle Regioni la potestà legislativa, salvo che per la determinazione di principi fondamentali, riservata alla legislazione dello Stato;
- ✓ in relazione a quanto precede spetta dunque alla Regione legiferare in materia di organizzazione del sistema sanitario regionale. Da qui la sua potestà decisionale di affidare ad un Ente pubblico strumentale, dipendente da questa, le funzioni di supporto tecnico scientifico alla Giunta ed al Consiglio regionale in materia di epidemiologia e verifica della qualità dei servizi sanitari; per l'esercizio di tali funzioni ARS è autorizzata con legge all'acquisizione di dati ovunque collocati a livello regionale, definendo, altresì, le operazioni eseguibili;

Tali argomentazioni furono accolte dal Garante e, quindi, dal Governo, in quanto fu ritenuta assolutamente legittima la scelta operata dal governo regionale. A seguito di tale chiarimento la legge regionale è stato promulgata.

2.3.2 Documento Programmatico sulla sicurezza.

Il documento programmatico per la sicurezza (d'ora in avanti "DPS") è una "misura minima" prevista dalla legge e si traduce in un rapporto di analisi contenente la distribuzione dei compiti, l'analisi dei rischi sul trattamento dei dati e la documentazione di alcune soluzioni adottate ed altro ancora.
In base al nuovo Codice della privacy, la misura minima del DPS deve essere adottata dal titolare di un trattamento di dati sensibili o giudiziari effettuato con strumenti elettronici.
Il documento programmatico sulla sicurezza non deve essere inviato a nessun ente e nemmeno al Garante per la Privacy. Andrà conservato presso l'ARS – Gruppo Privacy - e verrà esibito in caso di richiesta da parte degli organi di verifica (Guardia di Finanza).
In ottemperanza a quanto previsto dall'art. 34 del Codice della privacy, che elenca le misure minime di sicurezza da applicare, e dal disciplinare tecnico in materia di misure minime di sicurezza (allegato B, regola 19), che detta le modalità tecniche da adottare a cura del titolare, del responsabile e dell'incaricato in caso di trattamento

con strumenti elettronici, **l'ARS , in quanto titolare di trattamenti di dati sensibili e giudiziari effettuati con l'ausilio di strumenti elettronici, è tenuta a redigere un documento programmatico sulla sicurezza contenente una serie di informazioni essenziali previste dalla normativa. In particolare il DPS deve riguardare:**

- ✓ l'elenco trattamenti di dati personali
- ✓ la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati
- ✓ l'analisi dei rischi che incombono sui dati
- ✓ le misure da adottare per garantire l'integrità e la disponibilità dei dati e per proteggere aree e locali, ai fini della custodia e dell'accessibilità dei dati
- ✓ i criteri e le modalità per ripristinare la disponibilità dei dati in seguito a distruzione o danneggiamento
- ✓ i criteri per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti affidati all'esterno della struttura del titolare
- ✓ i criteri per la cifratura dei dati idonei a rilevare lo stato di salute e la vita sessuale o per la loro separazione dagli altri dati personali dell'interessato
- ✓ un programma di formazione degli incaricati al momento dell'ingresso in servizio e in occasione di cambiamenti di mansioni o di introduzione di nuovi strumenti rilevanti per il trattamento, relativamente ai rischi che incombono sui dati, alle misure disponibili per prevenire eventi dannosi, ai profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, alle responsabilità che ne derivano ed alla modalità per aggiornarsi sulle misure minime adottate dal titolare.

La normativa sulla privacy stabiliva che il documento così strutturato doveva essere adottato, in prima applicazione, entro il termine ultimo del **31 dicembre 2004**[26].

E' importante tuttavia sottolineare che il DPS costituisce un impegno costante dell'Agenzia, poiché:

- **deve essere aggiornato entro il 31 marzo di ogni anno,** in relazione:
  - ✓ alle innovazioni introdotte nel disciplinare tecnico di cui all'allegato B), del "Codice", relativo alle misure minime, che sarà aggiornato periodicamente con decreto del Ministro della giustizia di concerto con il Ministro per le innovazioni e le tecnologie, in relazione all'evoluzione tecnica e all'esperienza maturata nel settore;
  - ✓ ai mutamenti organizzativi e tecnologici che investono l'Agenzia;
- **ne deve essere data notizia nella relazione di accompagnamento al bilancio d'esercizio dell'ARS.**

L'Agenzia ha provveduto a tale adempimento approvando **il DPS con deliberazione CdA del 27 dicembre 2004, n. 35** "*Decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali) – Documento programmatico della sicurezza – Approvazione*".

[26] Il Codice dispone che il Titolare nei confronti dei Responsabili e questi ultimi nei confronti degli incaricati, devono dare istruzioni relativamente all'adozione delle misure minime di sicurezza previste, tra cui la predisposizione del Documento programmatico della sicurezza (entro il 30 giugno 2004 – Art. 180, comma 1). Detto termine, tuttavia è stato prorogato al 31 dicembre 2004, con decreto legge varato dal Governo in data 22 giugno 2004. Lo stesso decreto legge, all'art. 3, comma 2, differiva anche la scadenza prevista dall'art. 180, comma 3, del medesimo Codice, che riservava un margine di tempo ulteriore a tutti coloro che, pur gestendo dati personali attraverso strumenti elettronici, non erano in grado, per obiettivi ragioni tecniche, in tutto o in parte di applicare immediatamente le misure minime di sicurezza. La nuova scadenza era fissata al 31 marzo 2005.

L'adozione è avvenuta nel rispetto degli artt. 31,-36 del d.lgs. 196/2003 e del disciplinare tecnico di cui all'all. B del più volte citato "Codice"; per la redazione del DPS è stato fatto riferimento allo schema-tipo messo a disposizione dal Garante sul sito web ufficiale per facilitare l'adempimento dell'obbligo di redazione del medesimo. Lo stesso è stato aggiornato con successivi atti del titolare[27].

Il Gruppo privacy è tenuto alla conservazione del documento programmatico sulla sicurezza e deve assicurare al titolare ed ai responsabili del trattamento l'ausilio necessario per il suo aggiornamento.
Gli incaricati del trattamento sono tenuti a collaborare con il Gruppo Privacy al fine di segnalare le novità in relazione:

- ✓ **all'inizio di nuovi trattamenti;**
- ✓ **alla variazione o cessazione di determinati trattamenti;**
- ✓ **alle variazioni e allocazioni degli strumenti utilizzati per i trattamenti.**

Il Gruppo privacy e gli incaricati devono fare riferimento per le misure di sicurezza ai contenuti descritti nel DPS come aggiornato da ultimo con deliberazione CdA del 26 aprile 2007, n.11, disponibile sul portale Privacy in corso di allestimento.

2.3.3 Informativa all'interessato/ Consenso

Il "Codice" sviluppa il principio del bilanciamento degli interessi di tutela con uno snellimento degli adempimenti a carico degli Enti, poiché ai soggetti pubblici i trattamenti dei dati personali sono consentiti soltanto per lo svolgimento delle funzioni istituzionali (art. 18, co. 2), e poiché possono trattare solo i dati sensibili e giudiziari indispensabili per svolgere attività istituzionali che non possono essere adempiute mediante trattamento dati anonimi o comuni (art. 22, co. 3).

L'area del consenso risulta sostanzialmente confermata rispetto all'ordinamento previgente, con l'individuazione, tuttavia, di alcune ipotesi di esonero.

Rimane fermo l'adempimento dell'informativa all'interessato preventiva al trattamento di tutti dati.

ARS, ai sensi e per gli effetti della disciplina recata dalla già citata l.r. 40/2005 e ss.mm. e, specificatamente delle disposizioni recate dal Tit. VII, Capo I della medesima, è ente pubblico dipendente della Regione, **autorizzato al trattamento di dati sensibili per scopi di studio e ricerca, e per l'esercizio dell'attività amministrativa.**

2.3.3.1 Informativa all'interessato

L'informativa può essere fornita all'interessato sia per iscritto che verbalmente. Nel fornire l'informativa di cui all'articolo 13 i soggetti pubblici devono fare espresso riferimento:

[27] Deliberazione CdA del 3 aprile 2006, n. 7 concernente "Decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali) – Documento programmatico della sicurezza –Aggiornamento", con cui si è provveduto ad aggiornare il DPS in relazione ai mutamenti tecnologici ed organizzativi dell'Ente.
Deliberazione CdA del 26 aprile 2007, n. 11 "Decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali) – Documento programmatico della sicurezza – Aggiornamento 2007", con cui si è provveduto ad apportare modifiche ed integrazioni al DPS approvato con deliberazione 7/2006, a seguito del mutato quadro istituzionale ed organizzativo introdotto con la novellata disciplina dell'ARS di cui alla l.r. 10 luglio 2006, n. 28

- alla normativa che prevede gli obblighi o i compiti in base alla quale è effettuato il trattamento dei dati sensibili e giudiziari. Il trattamento può, comunque, riguardare solo i dati sensibili e giudiziari indispensabili per svolgere attività istituzionali che non possono essere adempiute, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa.
- le finalità del trattamento (ad esempio: ricerca scientifica e statistica, programma di ricerca biomedica o sanitaria ex art. 12/bis del d.lgs. 502/1992 e ss.mm., gestione del rapporto di lavoro, ecc.);
- le modalità di utilizzo dei dati personali raccolti e successivamente trattati (in modo automatico, tramite supporto elettronico, attraverso l'elaborazione di terzi, ecc.);
- l'indicazione dei diritti che l'interessato può esercitare in relazione al trattamento dei suoi dati (accesso, modifica, cancellazione, ecc.) ed il nominativo/denominazione sociale ed indirizzo del Titolare o del responsabile cui rivolgersi per l'esercizio dei predetti diritti;
- l'indicazione dei 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 del trattamento;
- l'obbligatorietà o meno del conferimento dei dati;
- le conseguenze di un eventuale rifiuto a fornire i dati;

L'informativa è sempre dovuta, a qualsiasi titolo l'ARS esegua il trattamento dei dati.

In merito all'obbligo di informativa si specifica che:

- ***ove l'ARS operi per scopi statistici o scientifici:*** gli stessi devono essere chiaramente determinati e resi noti all'interessato, unitamente alle informazioni descritte al paragrafo che precede. L'informativa viceversa non è dovuta quando richiede uno sforzo sproporzionato rispetto al diritto tutelato, se sono adottate le idonee forme di pubblicità individuate nei Codici di deontologia e di buona condotta[28] (Art. 105,c. 4 e art. 106 Codice); in particolare, il titolare adotta forme di pubblicità con le seguenti modalità:
  - ✓ *per trattamenti riguardanti insiemi numerosi di soggetti distribuiti sull'intero territorio nazionale*, inserzione su almeno un quotidiano di larga diffusione nazionale o annuncio presso un'emittente radiotelevisiva a diffusione nazionale;
  - ✓ *per trattamenti riguardanti insiemi numerosi di soggetti distribuiti su un'area regionale (o provinciale),* inserzione su un quotidiano di larga diffusione regionale (o provinciale) o annuncio presso un'emittente radiotelevisiva a diffusione regionale (o provinciale);
  - ✓ *per trattamenti riguardanti insiemi di specifiche categorie di soggetti, identificate da particolari caratteristiche demografiche e/o da particolari condizioni formative o occupazionali o analoghe*, inserzione in strumenti informativi di cui gli interessati sono normalmente destinatari.

  Inoltre, qualora il titolare ritenga di non utilizzare le forme di pubblicità sopraelencate, anche in considerazione della natura dei dati raccolti o delle modalità del trattamento, ovvero degli oneri che comportano rispetto al tipo di

[28] Codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e scientifici (Provvedimento del Garante n. 2 del 16 giugno 2004, Gazzetta Ufficiale 14 agosto 2004, n. 190)

ricerca svolta, il titolare medesimo può individuare idonee forme di pubblicità da comunicare preventivamente al Garante, il quale può, in ogni caso, prescrivere eventuali misure ed accorgimenti.

- ***ove l'ARS operi come organismo sanitario pubblico***: l'informativa si attua con modalità semplificata (cfr. art. 77, 79 e 81 del Codice). Il consenso al trattamento dei dati idonei a rivelare lo stato di salute, può essere manifestato con un'unica dichiarazione, anche oralmente. In tal caso il consenso è documentato, anziché con atto scritto dell'interessato, con annotazione dell'organismo sanitario pubblico;
- ***ove l'ARS operi come ente pubblico con trattamento di dati sensibili o giudiziaria di competenza della struttura amministrativa***, l'informativa è resa facendo espresso riferimento alla normativa che prevede gli obblighi o i compiti in base alla quale è effettuato il trattamento dei dati sensibili.

  Gli incaricati sono tenuti a fornire all'interessato per iscritto, antecedentemente o al momento della raccolta, l'informativa di cui all'art. 13 del Codice. Si veda al riguardo quanto precisato al successivo *paragrafo 2.3.3.3*.

- ***ove l'ARS operi come ente pubblico con trattamento di dati comuni (ovvero diversi da quelli sensibili)***, l'informativa è resa apponendo apposita clausola sugli atti amministrativi (bandi, avvisi pubblici, ecc), facendo espresso riferimento alle disposizioni del Codice. Si veda al riguardo quanto precisato al successivo *paragrafo 2.3.3.3*.

2.3.3.2 Consenso

Come già esplicitato i soggetti pubblici, ai sensi dell'art. 18, comma 4, **non devono richiedere il consenso dell'interessato.**

Per cui:

- nell'ambito della tipologia dell'attività svolta dall'Agenzia, per il trattamento di dati sensibili finalizzato a scopi di ricerca scientifica in campo medico, biomedico o epidemiologico qualora, come nel caso dell'Agenzia, appunto, la ricerca sia prevista da una disposizione di legge che prevede specificamente la tipologia dei dati e le modalità di trattamento, il combinato disposto degli articoli 18, comma 4 e 110, del Codice **esclude l'obbligo per i soggetti pubblici e, quindi per ARS, di richiedere il consenso;**
- analogamente per il trattamento di dati sensibili avente la finalità di tutela della salute riguardante un terzo o la collettività, ai sensi dell'articolo 76, comma 1, lett. b) del Codice il trattamento dei dati sensibili non richiede il consenso dell'interessato, ma la preventiva autorizzazione del Garante. **L'autorizzazione generale n. 2/2007, come in precedenza sottolineato, ha esonerato di fatto gli enti pubblici e, quindi l'ARS, dal richiedere la preventiva autorizzazione al Garante.**
- per il trattamento di dati sensibili e giudiziari nell'ambito delle attività afferenti alla struttura amministrativa, ove il trattamento sia dovuto per adempiere ad obblighi di legge o nel caso di trattamenti individuati da espressa disposizione di legge , **l'ARS non deve richiedere il consenso dell'interessato.**

l'ARS, qualunque sia la tipologia dell'attività svolta, non deve richiedere il consenso dell'interessato.

2.3.3.3. Modelli Informativa

Al fine di agevolare il lavoro degli incaricati, nei casi in cui ARS tratti dati **sensibili e giudiziari** sia per scopi statistici o scientifici, come organismo sanitario pubblico o per attività amministrative afferenti alla Direzione, si faccia riferimento all'allegato 2 "*Fac-simile Informativa*" che costituisce un'utile base di partenza da integrare e modificare in relazione alle finalità ed alle modalità del trattamento. Detti modelli-tipo, pertanto, devono essere utilizzati avendo riguardo di inserire gli elementi di pertinenza del trattamento *de quo*.

L'Allegato 2, a sua volta è articolato in due *"Fac-simile di Informativa":*
2/A "Fac-simile di Informativa" da utilizzare per progetti di studio e ricerca di cui è titolare ARS per i quali l'acquisizione dei dati avviene attraverso la raccolta diretta;
2/B "Fac-simile di Informativa" da utilizzare per progetti di studio osservazionale o di ricerca di cui è titolare ARS per i quali l'acquisizione di dati avviene attraverso la consultazione di cartelle cliniche e in relazione ai quali sono stati attivati i Comitati etici locali delle Azienda sanitarie.
Ove l'ARS operi come ente pubblico con trattamento di dati **comuni** (ovvero diversi da quelli sensibili e giudiziari), si faccia riferimento al *Fac-simile di clausola* descritta ***nell'allegato 3.***

2.3.4 Trasferimento dati all'estero

In materia di trasferimento dei dati all'estero le disposizioni del Codice tendono a bilanciare l'esigenza di non restringere o vietare la libera circolazione dei dati personali è la necessità di tutela della riservatezza in quei Paesi che non offrono al riguardo sufficienti garanzie.

Il Titolo VII, artt. 42-45 del "Codice" disciplina le modalità cui attenersi a seconda che il trasferimento dei dati avvenga:

- all'estero nei Paesi Terzi non appartenenti all'U.E.;
- all'estero nei Paesi dell'U.E.;

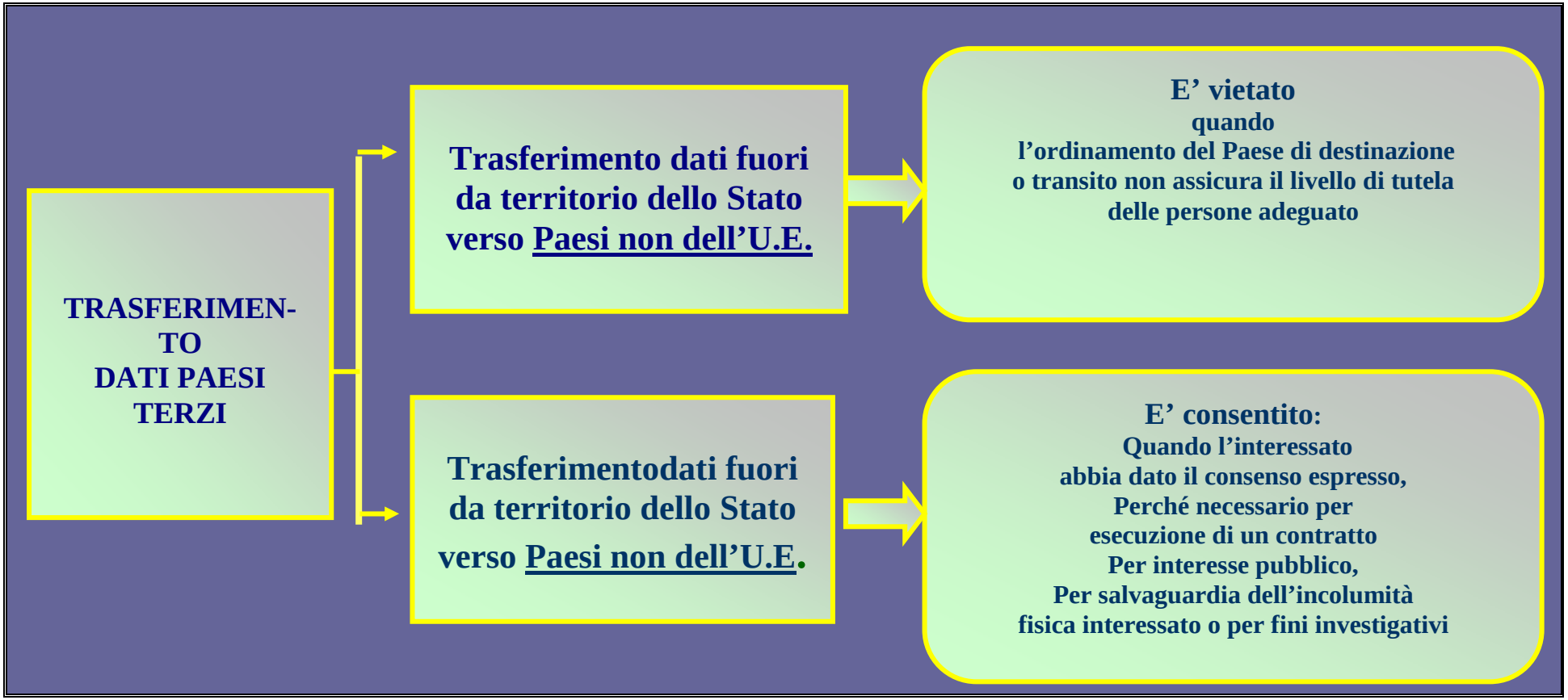
Le Tavole 4, 4-*bis* e 5 che seguono sintetizzano le disposizioni in parola, evidenziando i divieti imposti e le possibilità concesse dalla normativa di settore.

2.3.4.1 Trasferimento dati all'estero in Paesi Terzi non appartenenti all'U.E.

L'art. 43 del "Codice" disciplina le modalità per il trasferimento anche temporaneo fuori del territorio dello Stato, con qualsiasi forma o mezzo, di dati personali oggetto di trattamento, diretto verso un Paese non appartenente all'Unione europea, definendone i divieti e possibilità.

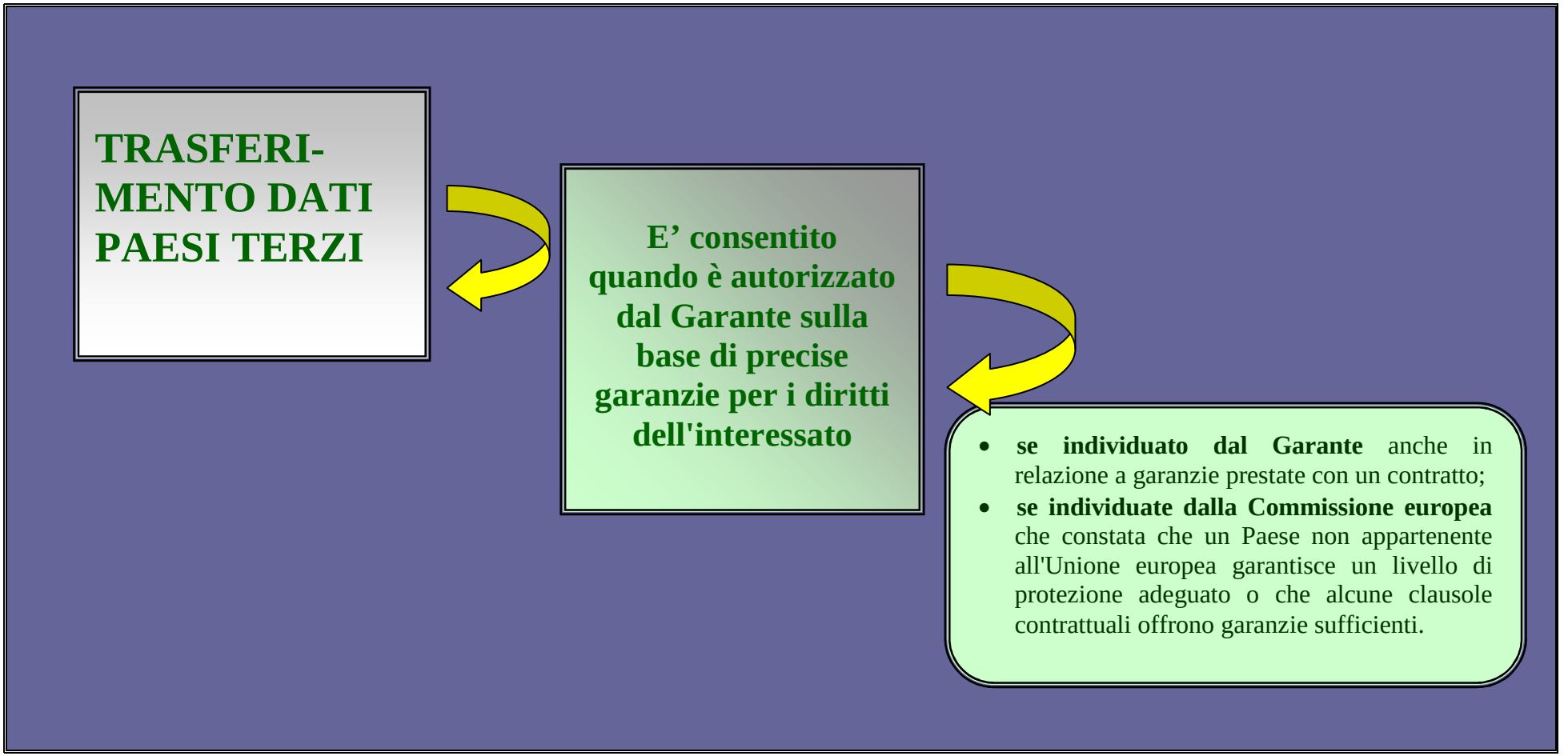
Lo schema che segue sintetizza la disciplina in materia:

Tav. 4



L'art. 44, poi , disciplina altri trasferimenti consentiti verso un **Paese non appartenente all'Unione Europea**
Lo schema che segue sintetizza la disciplina in materia:

Tav. *4/bis*

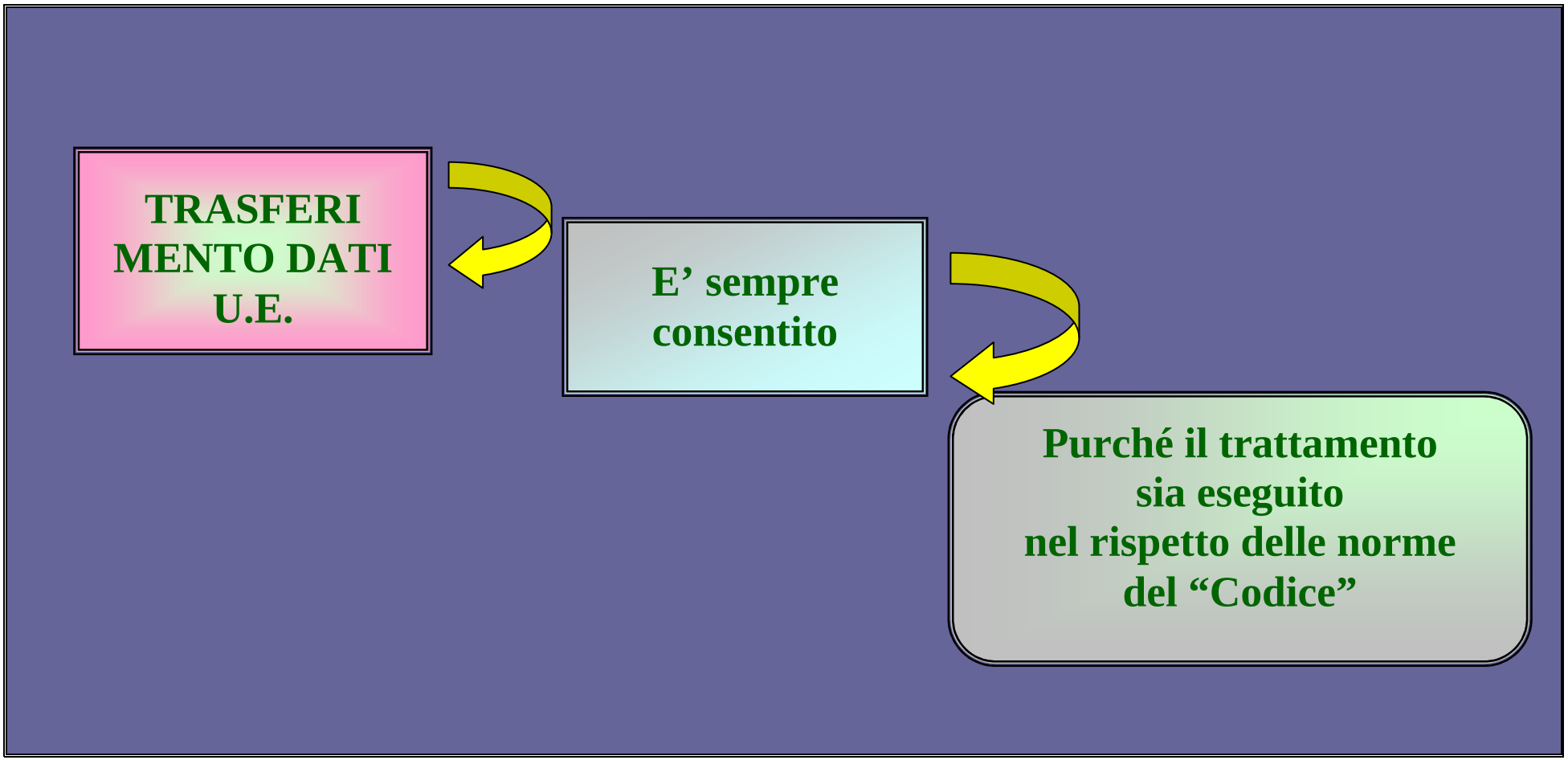


2.3.4.2 Trasferimento dati all'estero nei Paesi dell'U.E.

L'art. 42 precisa come le disposizioni del "Codice" non possono essere applicate in modo tale da restringere o vietare la libera circolazione dei dati personali **fra gli Stati membri dell'Unione europea**, fatta salva l'adozione, in conformità allo stesso Codice, di eventuali provvedimenti in caso di trasferimenti di dati effettuati al fine di eludere le medesime disposizioni.

Lo schema che segue sintetizza la disciplina in materia:

Tav. 5



2.3.5 Comunicazione dati all'interno dello Stato italiano da ente pubblico a ente pubblico o privato

L'art. 4 del "Codice" intende per "*comunicazione*"[29], 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.

Anche i soggetti pubblici sono tenuti ad osservare le disposizioni in materia di comunicazione e diffusione dei dati.

Il Codice, tuttavia, individua obblighi diversi a seconda che:

- si tratti dati comuni o dati sensibili e giudiziari;
- la comunicazione dei dati avvenga tra soggetti pubblici o tra quest'ultimi e soggetti privati.

2.3.5.1 La comunicazione da parte di un soggetto pubblico ad altro soggetto pubblico o privato di dati diversi da quelli sensibili e giudiziari

- **Comunicazione dei dati comuni ovvero diversi da quelli sensibili e giudiziari ad altri soggetti pubblici (art. 19, comma 2)**

La comunicazione da parte di un soggetto pubblico ad altri soggetti pubblici di dati diversi da quelli sensibili e giudiziari é ammessa solo quando è prevista da una norma di legge o di regolamento (art. 19, comma 2, del Codice). 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 decorso il termine di cui all'articolo 39, comma 2[30], e non sia stata adottata la diversa determinazione ivi indicata.

La comunicazione dei dati *de quo* è consentito per ARS in quanto previsto da una norma di legge e necessaria per lo svolgimento delle proprie funzioni istituzionali[31].

---

[29] La comunicazione differisce dalla diffusione. Al riguardo si faccia riferimento a quanto precisato nel Cap. 1, paragr. 1.2.

[30] **Articolo 39. Obblighi di comunicazione**.

1. Il titolare del trattamento è tenuto a comunicare previamente al Garante le seguenti circostanze:

a) comunicazione di dati personali da parte di un soggetto pubblico ad altro soggetto pubblico non prevista da una norma di legge o di regolamento, effettuata in qualunque forma anche mediante convenzione;

b) trattamento di dati idonei a rivelare lo stato di salute previsto dal programma di ricerca biomedica o sanitaria di cui all'articolo 110, comma 1, primo periodo.

2. I trattamenti oggetto di comunicazione ai sensi del comma 1 possono essere iniziati decorsi quarantacinque giorni dal ricevimento della comunicazione salvo diversa determinazione anche successiva del Garante.

3. La comunicazione di cui al comma 1 è inviata utilizzando il modello predisposto e reso disponibile dal Garante, e trasmessa a quest'ultimo per via telematica osservando le modalità di sottoscrizione con firma digitale e conferma del ricevimento di cui all'articolo 38, comma 2, oppure mediante telefax o lettera raccomandata.

[31] Ai sensi dell'art. 82-*ter* della l.r. n. 40/2005 e ss.mm., ARS, per l'esercizio delle funzioni istituzionali può "*procedere all'acquisizione di dati, attraverso la raccolta diretta e sistematica e l'accesso a banche dati, nonché alla loro elaborazione, pubblicazione e diffusione nei limiti e con le garanzie previsti dal decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali) e dalla legge regionale 3 aprile 2006, n. 13 (Trattamento dei dati sensibili e giudiziari da parte della Regione Toscana, aziende sanitarie, enti, aziende e agenzie regionali e soggetti pubblici nei confronti dei quali la Regione esercita poteri di indirizzo e di controllo)*".

- **Comunicazione dei dati comuni ovvero diversi da quelli sensibili e giudiziari da parte di un soggetto pubblico a soggetti privati o a enti pubblici economici (art. 19, comma 3)**

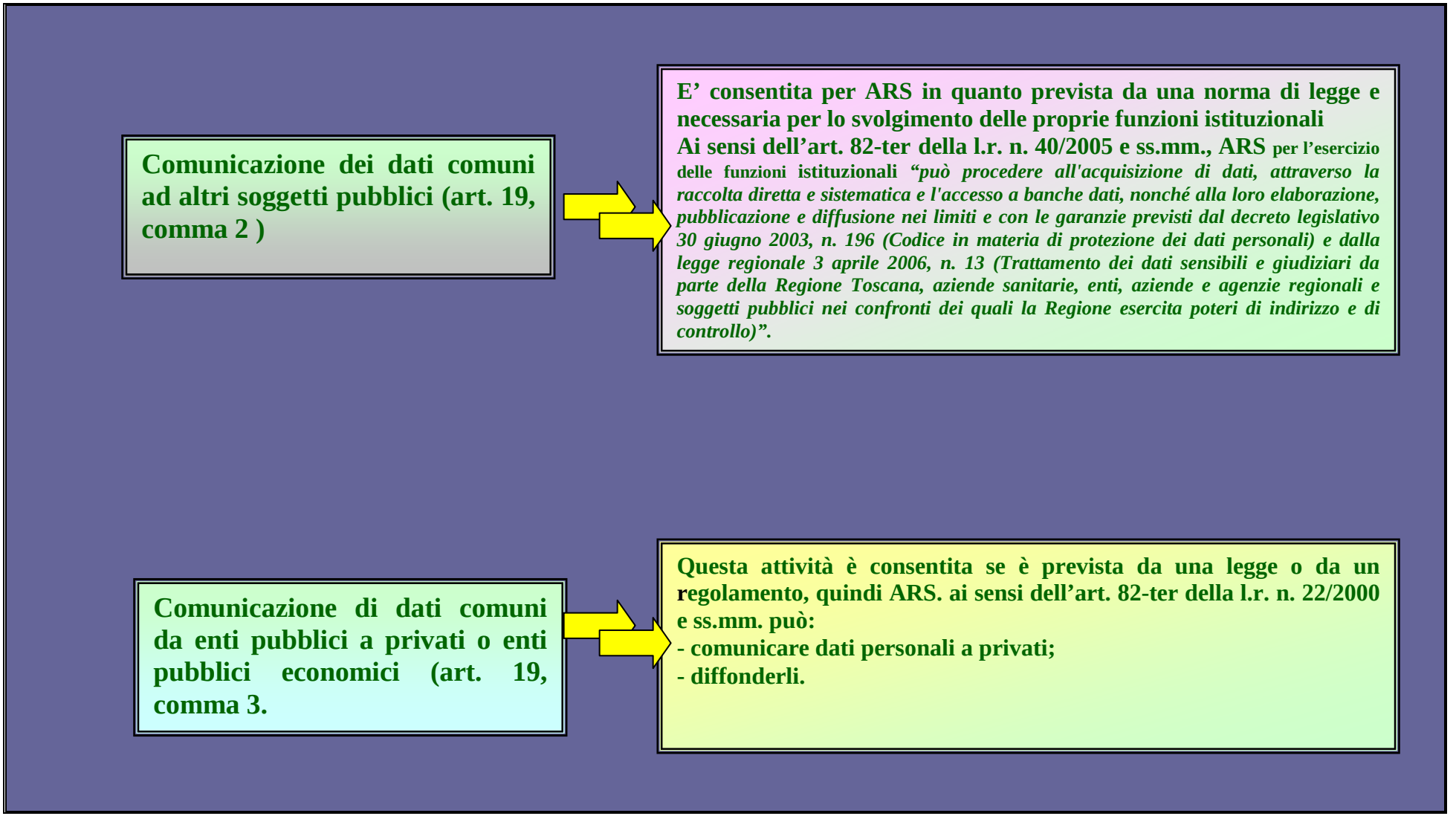
La comunicazione a privati o a enti pubblici economici e la diffusione sono ammesse unicamente quando sono previste da una norma di legge o di regolamento.
In ogni caso, non possono essere comunicati o diffusi i dati per i quali è stata ordinata la cancellazione, ovvero quando è stato superato il periodo di tempo necessario al raggiungimento degli scopi, ovvero per scopi diversi da quelli indicati nella notificazione del trattamento al Garante, ove prescritta.
La comunicazione dei dati *de quo* è consentito per ARS in quanto previsto da una norma di legge. ARS. ai sensi dell'art. 82-*ter* della l.r. n. 40/2005 e ss.mm. può:

- comunicare dati a privati;
- diffonderli.

La ***Tav. 6*** che segue sintetizza le disposizioni sopra illustrate:

2.3.5.1 La comunicazione da parte di un soggetto pubblico ad altro soggetto pubblico o privato di dati diversi da quelli sensibili e giudiziari

Tav. 6



2.3.5.2 La comunicazione da parte di un soggetto pubblico a altro soggetto pubblico o privato di dati sensibili e giudiziari

La comunicazione da parte di un soggetto pubblico ad altro soggetto pubblico o privato **di dati sensibili e giudiziari** é regolata dal combinato disposto di cui all'art. 18, comma 5 e art. 25 del Codice, con il quale si disciplinano i soli divieti di *comunicazione e diffusione.*

In particolare la comunicazione e la diffusione sono vietate, oltre che in caso di divieto disposto dal Garante o dall'autorità giudiziaria, limitatamente alle seguenti circostanze:

- ***in riferimento a dati personali dei quali è stata ordinata la cancellazione***, ***ovvero quando è decorso il periodo di tempo indicato dall'art. 11, comma 1, lettera e)***, ovvero quando è decorso il periodo di liceità del trattamento (o più precisamente decorso il periodo utile ad eseguire il trattamento dei dati sensibili o giudiziari in una forma che consenta l'identificazione dell'interessato, che deve essere limitato al tempo necessario agli scopi per i quali i dati stessi sono stati raccolti o successivamente trattati);
- ***per finalità diverse da quelle indicate nella notificazione del trattamento,*** ove prescritta.

<u>La comunicazione dei dati *de quo* è consentita per ARS in quanto la stessa è autorizzata:</u>

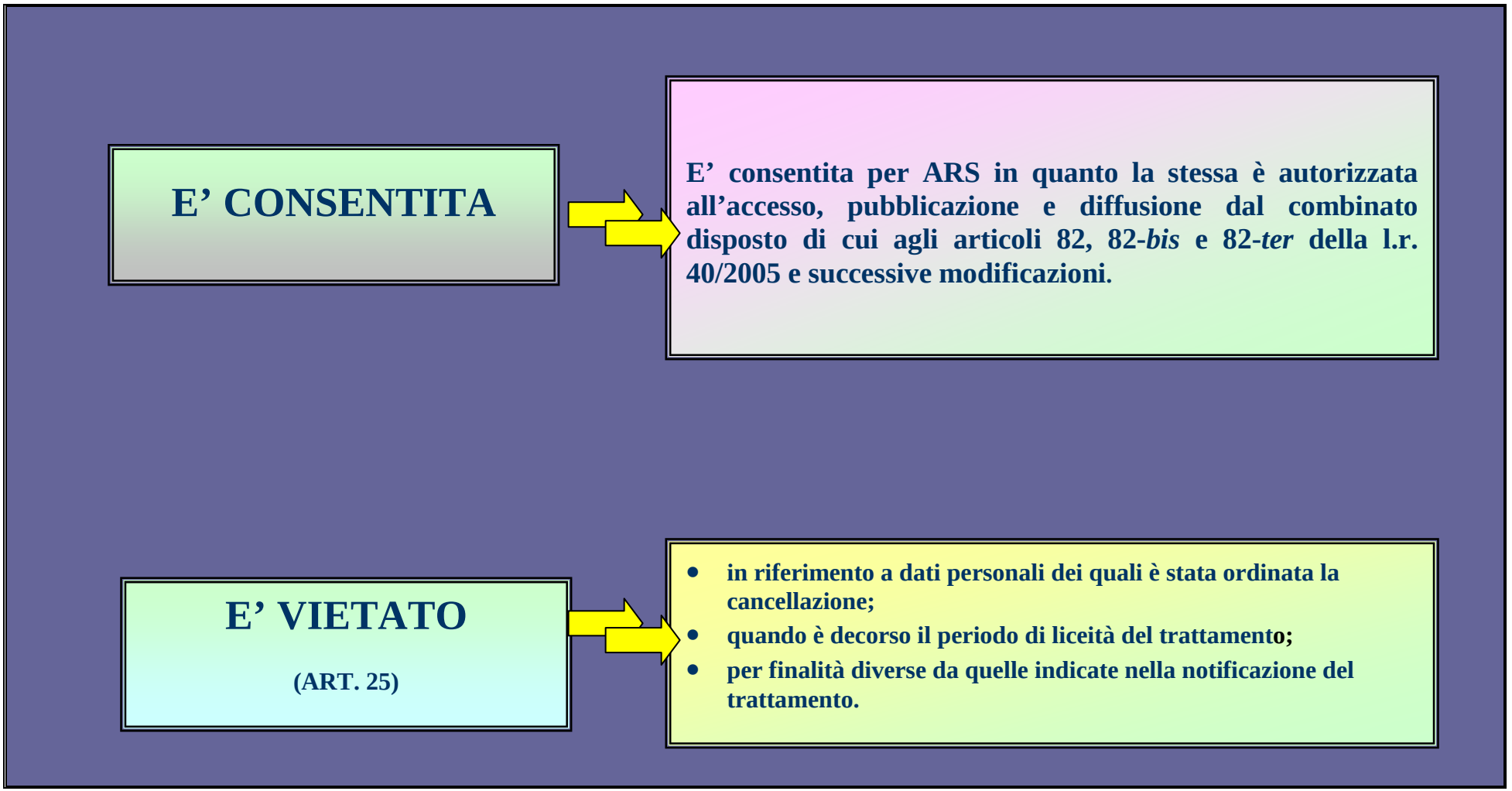
- ✓ <u>all'accesso, pubblicazione e diffusione dal combinato disposto di cui agli articoli 82, 82-*bis* e 82-*ter* della più volte citata l.r. 40/2005 e successive modificazioni, per attività di studio e ricerca afferenti alle strutture scientifiche;</u>
- ✓ <u>alla comunicazione per effetto di specifica disciplina per attività afferenti alla Direzione (cfr. Capo III, paragrafo 3.4. – Tabelle da 12 a 22).</u>

<u>Gli incaricati, comunque, dovranno rispettare le disposizioni del "Codice" in ordine ai divieti richiamati al paragrafo che precede.</u>

La ***Tav. 7*** che segue sintetizza le disposizioni sopra illustrate.

2.3.5.2 La comunicazione da parte di un soggetto pubblico a altro soggetto pubblico o privato di dati sensibili e giudiziari

Tav. 7



2.3.5.3 Modelli per comunicazione dati

Di seguito sono elencati gli allegati al presente paragrafo, che presentano i vari modelli da utilizzare per effettuare le comunicazioni sopra indicate.
Occorre tuttavia evidenziare il carattere volutamente generale degli stessi, essi rappresentano un contributo di accompagnamento alle strutture che dovrà essere adeguato alle circostanze concrete di utilizzo.

- ***All. 4*** – **Fac-simile di istanza per richiedere i dati ad altro ente pubblico o privato, articolato in:**
  - ✓ ***4/A - Fac- simile di istanza per richiesta dati da parte degli Osservatori;***
  - ✓ ***4/B - Fac -simile di istanza per richiesta dati da parte della Direzione.***
- ***All. 5*** – **Fac-simile di lettera per trasmissione dati da ARS a ente pubblico o privato.**

2.3.6 Diffusione di dati

Per "*diffusione*", s'intende il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
L'art. 25 del Codice, in analogia a quanto già disposto in materia di "*trasferimento dei dati*", disciplina i divieti per la diffusione dei dati personali. E' ragionevole pensare che, esclusi i casi di divieto espressamente indicati dal Codice, di cui daremo conto di seguito, la diffusione in analogia alla comunicazione è generalmente consentita agli enti pubblici (art. 18, comma 5).
Tale assunto trova per ARS maggior conferma nella circostanza che la legge istitutiva, art. 82-*ter*, comma 2, lett. b), autorizza l'Ente, nell'ambito delle materie e compatibilmente con i compiti istituzionali, ad acquisire notizie e documentazioni, utilizzando anche i dati degli enti, agenzie e fondazioni regionali; procedere all'acquisizione di dati, attraverso la raccolta diretta e sistematica e l'accesso a banche dati, nonché alla loro elaborazione, pubblicazione e, appunto, diffusione nei limiti e con le garanzie previsti dal "Codice".
Gli incaricati al trattamento dovranno, tuttavia, rispettare i divieti espressamente indicati dal Codice. Il divieto di comunicazione e diffusione, infatti, oltre che in caso di divieto disposto dal Garante o dall'autorità giudiziaria è previsto:

- ***in riferimento a dati personali dei quali è stata ordinata la cancellazione, ovvero quando è decorso il periodo di tempo di liceità del trattamento;***
- ***per finalità diverse da quelle indicate nella notificazione del trattamento.***

Il Codice prevede, inoltre particolari garanzie per i dati idonei a rilevare lo stato di salute. L'art. 22, comma 8, infatti, dispone il divieto della diffusione di detti dati.

2.3.6.1 Diffusione dei dati personali sensibili tramite pubblicazione sul BURT

Con espresso riferimento alle attività afferenti alla struttura tecnico-amministrativa (Direzione), non può valere il disposto di cui all'art. 82-*ter* della l.r. 40/2005 e ss.mm.,

in quanto riferito alle attività di studio e ricerca proprie delle strutture scientifiche (Osservatori).
La diffusione dei dati personali sensibili è ammessa solo se prevista da espressa e specifica disposizione di legge (art. 22, comma 11, Codice).
In assenza di una precisa previsione normativa, pertanto, non è consentita la diffusione tramite pubblicazione sul BURT degli atti amministrativi che contengono dati sensibili con specifico riguardo alla diffusione dei dati idonei a rilevare lo stato di salute; tali atti sono qualificati riservati e pubblicai solo per estremi (art. 26, comma 5, Codice). Gli incaricati della Direzione, pertanto, dovranno avere cura di verificare la sussistenza di una specifica previsione normativa che consenta la diffusione di tali dati.

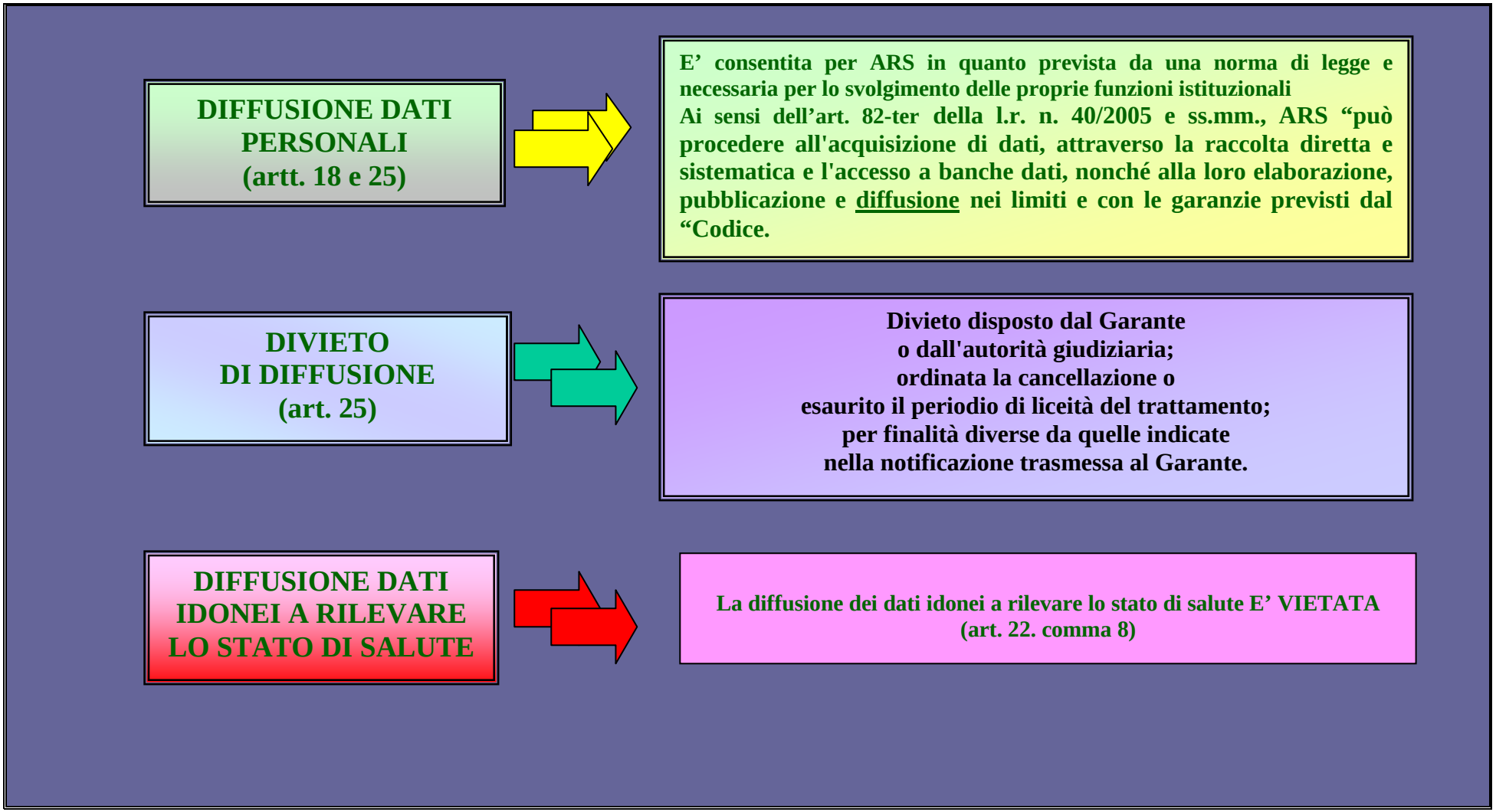
2.3.6.2 Diffusione dei dati giudiziari tramite pubblicazione sul BURT

Per la diffusione dei dati giudiziari tramite BURT valgono le stesse indicazioni fornite peri dati personali sensibili al precedente punto 2.3.6.1.

La ***Tav. 8*** che segue sintetizza le disposizioni sopra illustrate.

Diffusione dati personali

Tav. 8



2.3.7 Affidamento trattamenti dati all'esterno

In caso di affidamento all'esterno del trattamento di dati, si applicano le seguenti disposizioni:

1. agli Enti, agli organismi, agli altri soggetti esterni all'ARS ed alle strutture accreditate, con esclusivo riferimento alle connesse operazioni di trattamento di dati, è attribuita la qualità di Responsabile ai sensi dell'art. 29 del "Codice";
2. i rapporti intercorrenti fra ARS e soggetti esterni sono regolati come segue:
   a) in caso di affidamento di trattamento di dati personali a Enti pubblici o Aziende sanitarie, mediante stipula di apposita convenzione/protocollo d'intesa, **gli incaricati della struttura amministrativa competente dovranno avere cura di definire nell'atto medesimo, previa intesa con ciascun Responsabile del trattamento:**
      1. che il trattamento dei dati avverrà sulla base d'intese che intercorreranno fra i Responsabili del trattamento degli Enti firmatari;
      2. che l'ente firmatario s'impegna a sottoscrivere la clausola contemplata al punto 3;
   b) in caso di affidamento a Ditta esterna mediante la stipula di apposito contratto, gli incaricati della struttura amministrativa dovranno avere cura di inserire nell'atto medesimo l'impegno da parte della Ditta affidataria a sottoscrivere la clausola di cui al punto 3.
3. Negli accordi con le strutture accreditate e nei contratti di affidamento di attività o di servizi all'esterno dell'Agenzia *(outsourcing)* deve essere inserita apposita clausola di garanzia, di cui al modello illustrato al paragrafo che segue, in cui l'Ente/soggetto cui sono affidati i dati di cui è titolare ARS s'impegna all'osservanza delle norme di legge sulla protezione dei dati personali e ad osservare quanto disposto dall'ARS in materia di trattamento di dati personali, effettuati in forza del rapporto convenzionale/contrattuale.

In sede di prima applicazione delle presenti prescrizioni, gli incaricati della strutture competente per la stipula e la conservazione delle convenzioni, protocolli d'intesa e contratti effettua una ricognizione della situazione in essere, al fine di provvedere agli adempimenti di legge.
Copia di tali atti dovrà essere inviata al referente del Gruppo Privacy ai fini:

- della tenuta e aggiornamento del CE.TRA. di cui al successivo paragr. 2.5.2;
- della tenuta e dell'aggiornamento del Registro delle convenzioni/contratti attraverso cui sono stati affidati trattamenti all'esterno di dati di cui è titolare l'ARS di cui al successivo paragr. 2.5.5.

2.3.7.1 Modelli per affidamento trattamento dati all'esterno

Il Garante evidenzia che occorre indicare le attività affidate a terzi che comportano il trattamento di dati, con l'indicazione sintetica del quadro giuridico o contrattuale (nonché organizzativo e tecnico) in cui tale trasferimento si inserisce, in riferimento agli impegni assunti, anche all'esterno, per garantire la protezione dei dati stessi.
Occorre, quindi:

- **indicare** la società, l'ente o il consulente cui è stata affidata l'attività e il ruolo ricoperto agli effetti della disciplina sulla protezione dei dati personali (titolare o responsabile del trattamento)
- **descrivere** gli impegni assunti dal terzo in ordine:
  - al trattamento di dati ai soli fini dell'espletamento dell'incarico ricevuto;
  - all'adempimento degli obblighi previsti dal Codice per la protezione dei dati personali;
  - al rispetto delle istruzioni specifiche eventualmente ricevute per il trattamento dei dati personali o integrazione delle procedure già in essere;
  - all'impegno a relazionare periodicamente sulle misure di sicurezza adottate;
  - ad informare immediatamente il titolare del trattamento in caso di situazioni anomale o di emergenze.

Le regole da seguire per l'affidamento del trattamento dati all'esterno sono le seguenti:

- ***Descrizione dell'attività "esternalizzata"***: indicare sinteticamente l'attività affidata all'esterno;
- ***Trattamenti di dati***: indicare i trattamenti di dati, sensibili o giudiziari, effettuati nell'ambito della predetta attività;
- ***Soggetto esterno***: indicare la società, l'ente o il consulente cui è stata affidata l'attività, e il ruolo ricoperto agli effetti della disciplina sulla protezione dei dati personali (titolare o responsabile del trattamento);
- ***Descrizione dei criteri***: perché sia garantito un adeguato trattamento dei dati è necessario che la società a cui viene affidato il trattamento rilasci specifiche dichiarazioni o documenti, oppure assuma alcuni impegni anche su base contrattuale, con particolare riferimento, ad esempio, a:
  - trattare i dati ai soli fini dell'espletamento dell'incarico ricevuto;
  - adempiere agli obblighi previsti dal Codice per la protezione dei dati personali;
  - rispettare le istruzioni specifiche eventualmente ricevute per il trattamento dei dati personali o integrazione delle procedure già in essere;
  - impegnarsi a relazionare periodicamente sulle misure di sicurezza adottate – anche mediante eventuali questionari e liste di controllo- e ad informare immediatamente il titolare del trattamento in caso di situazioni anomale o di emergenze.

I modelli da utilizzare per effettuare l'affidamento del trattamento dei dati all'esterno sono rintracciabili nei seguenti allegati:

- ***All. 6*** *"Clausola da inserire negli accordi con Enti e strutture accreditate e nei contratti di affidamento di attività o di servizi all'esterno dell'Agenzia (outsourcing)";*
- ***All. 7*** *"Modello per affidamento trattamento dati all'esterno".*

Occorre tuttavia evidenziare il carattere volutamente generale dei modelli proposti, che rappresentano solo un contributo di accompagnamento alle strutture, con l'avvertenza che gli stessi dovranno necessariamente essere adeguati alle circostanze concrete di utilizzo.

2.4 Tabelle riassuntive adempimenti ARS

Al fine di facilitare il compito degli incaricati, i paragrafi 2.2. e 2.3 che precedono, sono completati da tabelle riassuntive degli adempimenti a rilevanza esterne da adempiere nei confronti del Garante e degli adempimenti rilevanti da attuare nel rispetto della più generale disciplina recata dal Codice, tenuto conto della diversa natura di operare dell'ARS.
La lettura delle tabelle che seguono deve essere, comunque, operata avendo a riferimento quanto in precedenza illustrato.

ARS nella veste di Ente pubblico che opera per scopi di ricerca scientifica e statistica
(Strutture scientifiche - Veste più ricorrente)
Tab. 4

TIPOLOGIA	AUTORIZZAZIONE GARANTE (Art. 20)	NOTIFICAZIONE AL GARANTE (Artt. 37, co. 1, lett. b e 38[32]	COMUNICAZIONE AL GARANTE (Art. 39, co. 1, lett. b)[33]	CONSENSO INTERESSATO (Art. 110)	INFORMATIVA INTERESSATO (Artt. 13,105, 106, co.1, lett. b)	REGOLAMENTO DATI (Art. 20)	DOCUMENTO PROGRAMMATICO SICUREZZA[34] (Art. 34, co. 1, lett. g) e All. B)
TRATTAMENTO DATI SENSIBILI PER SCOPI STATISTICI O SCIENTIFICI[35] **Ricerca medica, biomedica ed epidemiologica**	**NO**	**SI**	**SI** *trattamento di dati idonei a rilevare lo stato di salute della popolazione previsto dai programmi di ricerca biomedica e sanitaria di cui all'art. 12- bis d.lgs. 502/1992 e succ. modif.*	**NO**[36]	**SI,** *gli scopi statistici o scientifici devono essere chiaramente determinati e resi noti all'interessato*[37]*.*	**SI** *ove si tratti dati diversi da quelli identificati nella legge istitutiva.*	**SI**

[32] La notificazione è presentata al Garante prima di ogni trattamento ed una sola volta a prescindere dal numero delle operazioni e dalla durata del trattamento e può riguardare uno o più trattamenti con finalità correlate. La notificazione è valida solo se trasmessa per via telematica utilizzando il modello predisposto dal Garante.

[33] La comunicazione è inviata utilizzando il modello predisposto e reso disponibile dal Garante, e trasmessa, a quest'ultimo per via telematica, osservando le modalità di sottoscrizione con firma digitale e conferma del ricevimento della notificazione (artt. 38 e 39 "Codice").

[34] Il DPS doveva essere adottato dal Titolare del trattamento, anche su proposta del Responsabile, entro il 30 dicembre 2004, così come disciplinato dal decreto legge varato dal Governo il 22 giugno 2004. L'ARS ha già provveduto con deliberazione del CdA n. 35 del 27 dicembre 2004. A regime, lo stesso deve essere aggiornato entro il 31 marzo di ogni anno in relazione all'evoluzione tecnica e all'esperienza maturata nel settore, secondo le decisioni adottate con Decreto del Ministro di grazia e giustizia assunte di concerto con il Ministro per le innovazioni e le tecnologie. ARS ha provveduto ai successivi aggiornamenti. Dell'adozione e aggiornamento del DPS deve essere data notizia nella relazione di accompagnamento al bilancio d'esercizio dell'Ente.

[35] Il trattamento di dati sensibili per scopi statistici o scientifici è soggetto alla disciplina del Codice di deontologia e di buona condotta di cui all'art. 106 "Codice".

[36] Quando la ricerca è prevista da espressa disposizione di legge (ed è il caso dell'ARS), ovvero rientra in un programma di ricerca biomedica e sanitaria previsto dall'art. 12- *bis* d.lgs. 502/1992 e successive modificazioni.

[37] L'informativa all'interessato non è dovuta quando richiede uno sforzo sproporzionato rispetto al diritto tutelato, se sono adottate le idonee forme di pubblicità individuate nei Codici di deontologia e di buona condotta (Art. 105, c. 4 e Art. 106 "Codice").

ARS nella veste di Ente pubblico che opera in qualità di "Organismo sanitario pubblico
(Strutture scientifiche - Veste meno ricorrente)

Tab. 5

TIPOLOGIA	AUTORIZ-ZAZIONE GARANTE (Art. 76, co. 1, lett. b)	NOTIFICAZIONE AL GARANTE (Artt. 37, co. 1, lett. b) e 38)	COMUNICAZIONE AL GARANTE (Art. 39, co. 1, lett. b)	CONSENSO INTERESSATO (Art. 76, co. 1, lett. b)	INFORMATIVA INTERESSATO (Artt. 77 e 79)	REGOLA-MENTO DATI (Art. 20)	DOCUMENTO PROGRAMMA-TICO SICUREZZA (Art. 34, co. 1, lett. g) e All. B)
ORGANISMO SANITARIO PUBBLICO L'ARS, ancorché non eroghi prestazioni sanitarie, rientra tra gli organismi sanitari pubblici qualora tratti dati di tipo sanitario per perseguire finalità d'interesse pubblico che riguardi un terzo o la collettività.	NO[38].	SI	SI *ove si tratti di trattamento di dati idonei a rilevare lo stato di salute previsto da un programma di ricerca biomedica o sanitaria di cui all'art. 12 bis del d.lgs. 502/'92 e successive modificazioni.*	NO	SI, *con modalità semplificata.*	SI, *ove si tratti dati diversi da quelli identificati nella legge istitutiva.*	SI

[38] Con l'autorizzazione generale 2/2005 e ss.mm., al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale, gli organismi sanitari pubblici, unitamente ad altri soggetti, sono stati esonerati dall'obbligo di richiedere la preventiva autorizzazione al Garante per il trattamento di dati sensibili ex art. 76, comma 1, lett. b) del Codice.

ARS nella veste di Ente pubblico che opera trattamento di dati sensibili e giudiziaria
(Direzione)

Tab. 6

TIPOLOGIA	AUTORIZ-ZAZIONE GARANTE (Art. 20)	NOTIFICA-ZIONE AL GARANTE (Artt. 37, co. 1, lett. b) e 38)	COMUNICA-ZIONE AL GARANTE (Artt. 39 e 110)	CONSENSO INTERESSATO (Artt. 18, co. 4 e 20)	INFORMATIVA INTERESSATO (Artt. 13 e 22)	REGOLA-MENTO DATI SENSIBILI (Art. 20)	DOCUMENTO PROGRAM-MATICO SICUREZZA (Art. 34, co. 1. lett. G) e All. B)
ENTE PUBBLICO Trattamento dati sensibili/giudiziari	**NO**[39]	**SI**	**SI** *nel caso di dati personali da parte di un soggetto pubblico ad altro soggetto pubblico non prevista da una norma di legge o di regolamento, effettuata in qualunque forma anche mediante convenzione.*	**NO**	**SI,** *facendo espresso riferimento alla normativa che prevede gli obblighi o i compiti in base alla quale è effettuato il trattamento dei dati sensibili.*	**SI** *ove si tratti dati utili per lo svolgimento delle funzioni istituzionali diversi da quelli individuati da specifica normativa.*	**SI**

[39] L'autorizzazione deve essere richiesta **solo** per quei trattamenti che non sono coperti dalle autorizzazioni generali n. 1/2007 (*Autorizzazione n. 1/2007 al trattamento dei dati sensibili nei rapporti di lavoro*) e n. 7 (*Autorizzazione n. 7/2007 al trattamento dei dati a carattere giudiziario da parte di privati, di enti pubblici economici e di soggetti pubblici*), **o nel caso in cui in Garante non proceda a rinnovare le autorizzazioni concesse.**

2.5 Gli strumenti di coordinamento, monitoraggio e aggiornamento delle attività in materia di privacy.

Si presentano, nei paragrafi che seguono, i principali strumenti di coordinamento, monitoraggio e aggiornamento delle attività in materia di privacy, che il CdA dell'ARS ha disposto per una corretta e attenta applicazione delle disposizioni del "Codice" con il duplice obiettivo di:

- adempiere agli obblighi normativi;
- favorire una costante crescita, all'interno dell'Agenzia, di una nuova cultura della riservatezza.

2.5.1 Gruppo Privacy

Con deliberazione n. 18 del 28/06/2004 il CdA ha istituito in seno all'Agenzia un gruppo di lavoro denominato "Gruppo Privacy", stante l'impatto trasversale del "Codice" la cui applicazione richiede una serie di adempimenti a rilevanza interna ed esterna ed un'approfondita attività di monitoraggio, attraverso il coinvolgimento di più soggetti, con competenze e formazione diversificati.
Con la medesima deliberazione il CdA ha disposto che la nomina del predetto "Gruppo Privacy" fosse attuata mediante decreto del responsabile della struttura tecnico-amministrativa, adottato sulla base delle designazioni dei rispettivi responsabili di struttura e settori individuati con la medesima deliberazione.

2.5.1.1 Nomina e composizione del Gruppo Privacy

Il Segretario Amministrativo, con Decreto n. 45 del 27 luglio 2004, ha proceduto alla nomina del Gruppo Privacy sulla base delle designazioni pervenute dai responsabili delle strutture/settori interessati.
Tale decreto è in corso di rivisitazione a seguito dei mutamenti organizzativi dell'Ente disposti dal CdA anche a seguito dell'entrata in vigore della nuova disciplina dell'ARS introdotta con la l.r. 28/2006 e ss.mm.
Il Gruppo rappresenta un elemento di novità rispetto al "Codice" sulla privacy, la cui costituzione si è imposta per motivi di opportunità strategica.
L'idea di far germinare in seno all'ARS un gruppo costituito da personale interno è apparsa come lo strumento più idoneo a promuovere un cambiamento di cultura e mentalità all'interno dell'Agenzia, utile per raggiungere tutti gli operatori che hanno il proprio riferimento all'interno del gruppo.
Infatti, si tratta di una struttura a carattere multidisciplinare, costituita da diverse professionalità (giuridiche, amministrative, organizzative, tecniche, informatiche, statistiche ecc.) a supporto dello svolgimento dei compiti prescritti dal Codice.
In qualità di referente del Gruppo Privacy, secondo il disposto del citato Decreto 45/2004 era stata nominata la dott.ssa Anna Serino – Responsabile dell'Area di Legislazione Sanitaria, che ha coordinato il Gruppo Privacy, fino al suo pensionamento, curando la predisposizione di tutti gli adempimenti urgenti previsti dal "Codice". Con successiva decretazione tale incarico sarà affidato all'Ing. Marco

Santini - Responsabile U.O. Sistemi Informatici. Successivamente il referente sarà scelto a rotazione tra i componenti del Gruppo medesimo con lo scopo di responsabilizzare tutti gli addetti.
Il Referente ha il compito di programmare, congiuntamente ai membri del Gruppo, le attività necessarie, di trasmettere a ciascun componente le comunicazioni e le informazioni necessarie ai fini degli adempimenti agli stessi spettanti, di controllare le azioni svolte, di relazionare ai Responsabili sulle attività effettuate.
Allo stato sulla base delle designazioni pervenute e per effetto della nomina di cui ai decreti sopra ricordati, il Gruppo Privacy risulta costituito come indicato nella ***Tab. 7*** che segue:

Tab. 7 – "GRUPPO PRIVACY"

STRUTTURE/SETTORI	NOMINATIVI
REFERENTE	***Marco Santini***
Direzione: U.O. Sistemi informatici	**Marco Santini**
Direzione: U.O. Personale e Convenzioni	**Daniele Lachi** **Sara Salti**
Direzione: U.O. Centro statistico elaborazione dati	**Simone Bartolacci**
Direzione: U.O. Tecnologie dell'informazione	**Roberto Berni**
Osservatorio Epidemiologia: **Osservatorio per la Qualità:** **Direzione:** **Area per lo studio e la ricerca del governo degli aspetti equitativi e la rilevanza economica dei bisogni sanitari.:**	**Monica da Fré/Alice Berti** **Francesca Collini/Monica Simonetti** **Francesco Innocenti**

2.5.1.2 Compiti del Gruppo Privacy e articolazioni di funzioni

In relazione agli obblighi di rilevanza interna ed esterna, riassunti nella ***Tab. 8*** che segue, derivanti dall'applicazione del nuovo "Codice" sulla privacy, il CdA ha attribuito al Gruppo Privacy precisi compiti:

Tab. 8 Obblighi a rilevanza interna ed esterna

OBBLIGHI A RILEVANZA INTERNA	OBBLIGHI A RILEVANZA ESTERNA
Adozione misure di sicurezza - Predisposizione documento programmatico della sicurezza.	Notificazione al Garante
	Comunicazione al Garante
	Richiesta autorizzazione al Garante
Tenuta e aggiornamento censimento dati (CE.TRA) anche ai fini dell'aggiornamento della notificazione al Garante	Obblighi di informativa all'interessato
Tenuta e aggiornamento anagrafe Responsabili e incaricati.	Trasferimento dati all'Estero
Tenuta e aggiornamento Registro convenzioni/protocolli/contratti sia per l'affidamento all'esterno del trattamento dei dati sensibili o di sistemi di sicurezza, sia per l'accesso da parte di ARS a flussi di dati ovunque collocati o per l'accesso da parte di altri enti ai dati di ARS.	Comunicazione dati da ente pubblico a ente pubblico o privato
Tenuta e aggiornamento "Portale Privcy"	Comunicazione/Diffusione dati

In relazione a quanto precede il Gruppo Privacy svolge, pertanto, i seguenti compiti:

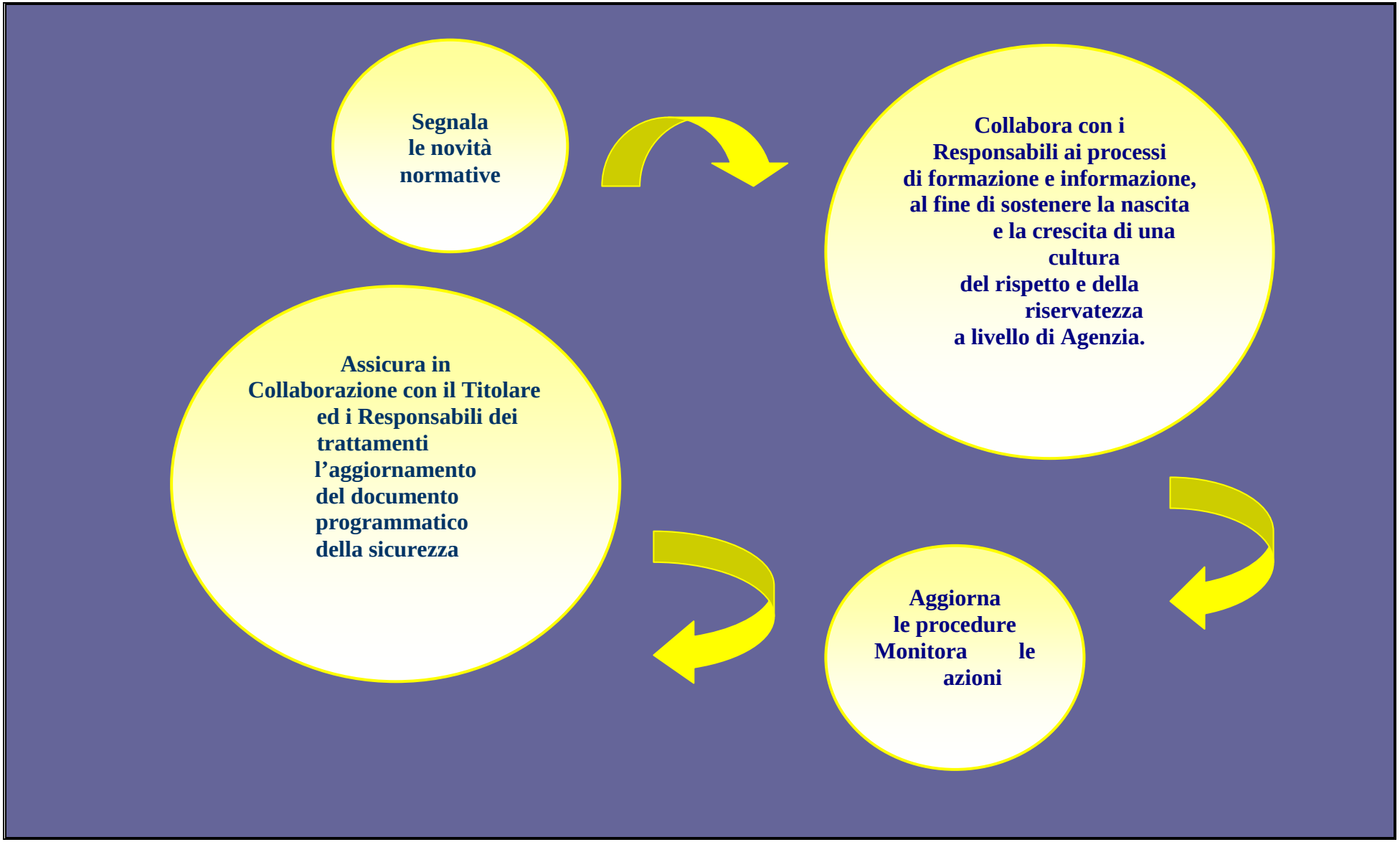
- segnala le novità normative;
- promuove, aggiorna e conserva:
  - la notificazione, le autorizzazioni (ove necessarie), le comunicazioni al Garante;
  - il censimento dei trattamenti dei dati personali sensibili/giudiziari (CE.TRA) sulla base delle comunicazioni effettuate dai Responsabili e dagli incaricati del trattamento e, in tale contesto, l'anagrafe dei Responsabili e degli incaricati;
  - l'elenco degli archivi cartacei e/o magnetici dei dati personali e/o sensibili/giudiziari custoditi dall'Agenzia;
  - il registro delle convenzioni/protocolli d'intesa/contratti relativi all'affidamento all'esterno del trattamento dei dati di cui è titolare ARS;
  - il registro delle convenzioni/protocolli d'intesa/ accordi /contratti stipulati con altri enti ai fini dell'accesso da parte dell'ARS a flussi di dati attinenti alla salute ovunque collocati o per l'accesso da parte di altri enti ai dati di ARS;
- aggiorna le procedure;
- assicura, in collaborazione con il Titolare ed i Responsabili dei trattamenti, l'aggiornamento del documento programmatico della sicurezza;

- collabora con i Responsabili ai processi di formazione e informazione, al fine di sostenere la nascita e la crescita di una cultura del rispetto e della riservatezza a livello di Agenzia;
- tiene ed aggiorna il "Portale Privacy".

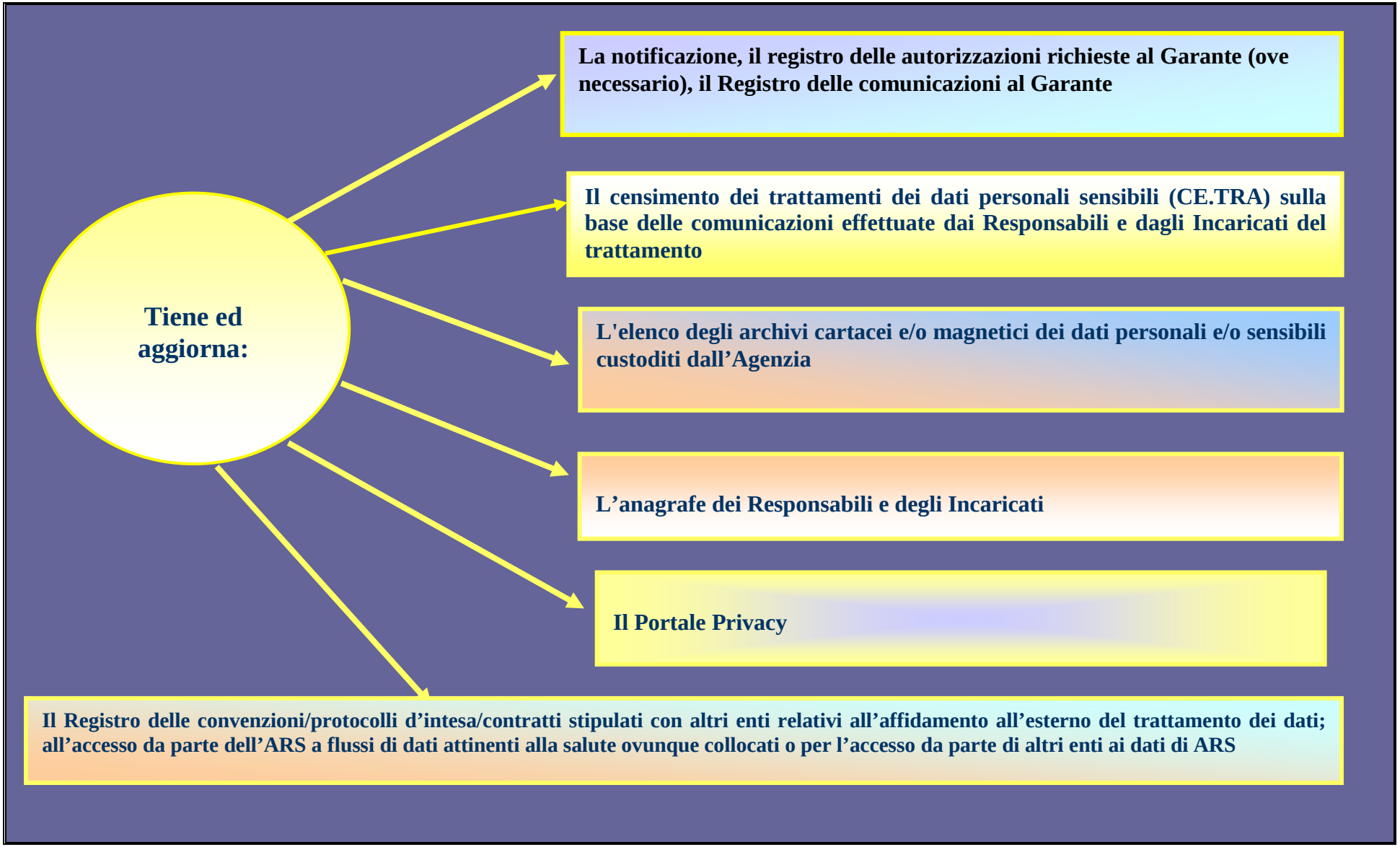
Al Gruppo sono, altresì, attribuiti compiti di monitoraggio con specifico riguardo alle tipologie di banche dati detenute, sia elettroniche sia cartacee, agli strumenti elettronici utilizzati per il trattamento (elaboratori stand-alone, computer collegati in rete locale, connessione a rete aperta ecc.),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

Le ***Tav. 9 e 9/bis*** che seguono offrono una sintesi grafica dei compiti attribuiti al Gruppo Privacy:

Tav. 9 - I compiti del Gruppo Privacy



Tav. 9/bis - I compiti del Gruppo Privacy



Il Gruppo Privacy ha articolato le proprie funzioni, attribuendo a ciascuno dei componenti precise attribuzioni, come identificate nella ***Tab. 9*** che segue:

Tab. 9 – Articolazioni funzioni in seno al Gruppo privacy

STRUTTURE/ SETTORI	NOMINATIVO	ATTIVITA'
REFERENTE	***Marco Santini***	▪ Coordinamento del Gruppo Privacy, con il compito di: - programmare, congiuntamente ai membri del Gruppo, le attività necessarie; - trasmettere a ciascun componente le comunicazioni e le informazioni necessarie ai fini degli adempimenti allo stesso spettanti; - controllare le azioni svolte, di relazionare ai Responsabili sulle attività effettuate. - sovrintendere alla gestione del Portale Privacy
DIREZIONE: U.O. Personale e Convenzioni	**Daniele Lachi**	▪ Tenuta e aggiornamento del Registro delle convenzioni/protocolli intesa/contratti relativi all'affidamento all'esterno del trattamento dei dati di cui è titolare ARS ▪ Tenuta e aggiornamento del registro delle convenzioni/protocolli d'intesa/ accordi /contratti stipulati con altri enti ai fini dell'accesso da parte dell'ARS a flussi di dati attinenti alla salute ovunque collocati o per l'accesso da parte di altri enti ai dati di ARS
	Sara Salti	▪ Assistenza giuridica in tutti i processi ▪ Segnalazione delle novità normative ▪ Aggiornamento notificazione ▪ Tenuta e aggiornamento registro autorizzazioni al Garante(ove necessarie) ▪ Tenuta e aggiornamento registro comunicazioni al Garante
DIREZIONE: U.O. Sistemi informatici	**Marco Santini**	▪ Aggiornamento delle procedure informatiche ▪ Stesura e l'aggiornamento del documento programmatico della sicurezza ▪ Monitoraggio degli strumenti elettronici utilizzati per il trattamento ▪ Monitoraggio delle banche dati sia elettroniche che cartacee ▪ Aggiornamento notificazione
DIREZIONE: U.O. Centro statistico elaborazione dati	**Simone Bartolacci**	▪ Tenuta e aggiornamento dell'anagrafe dei Responsabili e degli incaricati ▪ Tenuta e aggiornamento del censimento dei trattamenti dei dati personali sensibili (CE.TRA) sulla base delle comunicazioni effettuate dai Responsabili del trattamento ▪ Tenuta e aggiornamento dell'elenco degli archivi cartacei e/o magnetici dei dati personali e/o sensibili custoditi dall'Agenzia ▪ Monitoraggio dei flussi informativi verso l'esterno e quelli infra-strutture
DIREZIONE: U.O. Tecnologie dell'informazione	**Roberto Berni**	
OSS. EPIDEMIOLOGIA.: **OSS. PER LA QUALITA':** **Direzione: Area per lo studio e la ricerca del governo degli aspetti equitativi e la rilevanza economica dei bisogni sanitari:**	**Monica da Fré/Alice Berti** **Francesca Collini/Monica Simonetti** **Francesco Innocenti**	▪ Rapporti tra gli Osservatori ed il Gruppo Privacy ▪ Supervisione problematiche settori di pertinenza
Ognuno per il proprio ambito di competenza		▪ Collaborazione con i Responsabili ai processi di formazione e informazione, al fine di sostenere la nascita e la crescita di una cultura del rispetto e della riservatezza a livello di Agenzia. ▪ Gestione Portale Privacy

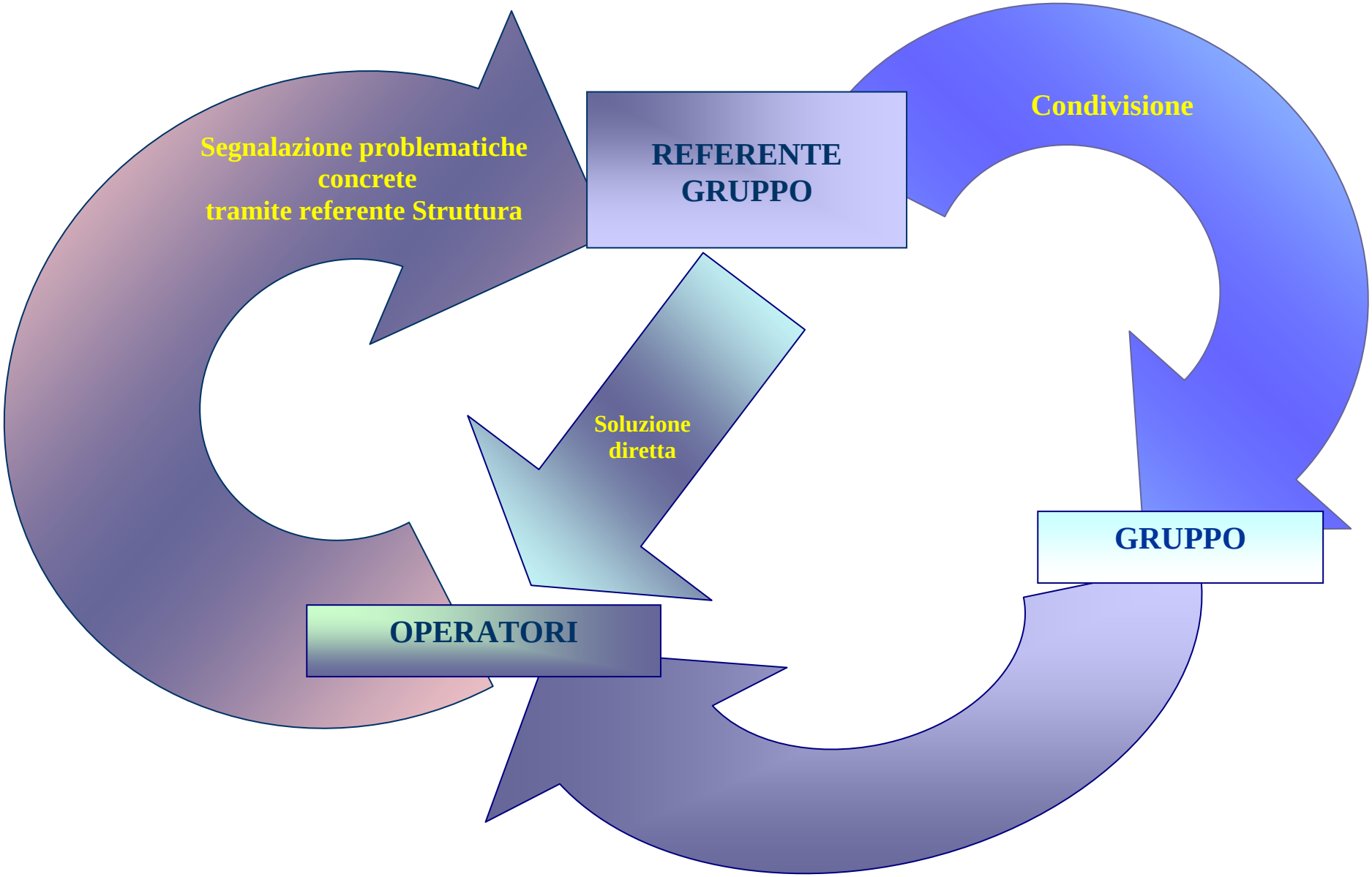
La funzione precipua del gruppo, dunque, si esplica nella diffusione della cultura privacy all'interno dell'Agenzia, sia attraverso l'attività istituzionale (intendendo con questa l'adempimento agli obblighi imposti dalla disciplina di legge), ma anche attraverso una costante azione di accompagnamento al sistema, con la risoluzione delle problematiche concrete, che quotidianamente emergono nell'esercizio dell'attività lavorativa.
Tale supporto sarà sostenuto in maniera più intensa nei primi mesi dalle istruzioni, per alleggerirsi progressivamente, a fronte del consolidamento delle conoscenze da parte di tutti gli operatori.
Del resto, il fine ultimo perseguito è quello di rendere tutto il personale ARS autonomo nella applicazione delle disciplina sulla privacy.
E' importante evidenziare che tale processo di acquisizione di conoscenze potrà essere attuato promuovendo il rispetto della privacy non tanto sul piano formale, ma sostanziale. In altri termini lo scopo che persegue il gruppo non è solo quello di applicare e far applicare le norme sulla privacy, ma quello di trasmettere che le stesse non siano un ulteriore impaccio burocratico, ma un miglioramento della qualità del lavoro svolto.
Il Gruppo ha altresì il compito di rendere meno gravosa l'attività scaturente dall'osservanza del Codice privacy, sia attraverso la semplificazione delle procedure tecniche ed informatiche, sia attraverso l'interpretazione del Codice in maniera molto ampia e tale da ridurre al minimo gli obblighi di legge.
Sotto profilo prettamente operativo, come in precedenza precisato, il Gruppo Privacy svolge funzione di **Monitoraggio**:
Oltre all'attività di monitoraggio i membri del Gruppo Privacy concorrono con i Responsabili del trattamento, anche alle attività di controllo interno, verificando la corrispondenza e la correttezza delle attività esercitate rispetto a quanto previsto in sede normativa e dalle presenti prescrizioni.

2.5.1.3 I rapporti tra gli incaricati ed il Gruppo Privacy

Il processo di consolidamento della cultura privacy impone ai referenti di ogni struttura di controllare l'esatto adempimento delle prescrizioni in materia, per cui a fronte di una palese violazione da parte di alcuno degli incaricati, si troverà a dover correggere eventuali errori o distrazioni dei medesimi.
Con tale funzione si vuol descrivere il particolare rapporto che dovrà instaurarsi tra il gruppo e gli incaricati del trattamento.
Infatti, questi ultimi, conoscendo le caratteristiche dei trattamenti di dati di propria competenza e le problematiche conseguenti, dovranno rapportarsi al Gruppo, tramite il proprio referente, per informarlo in modo completo delle questioni emerse al fine di individuare le soluzioni necessarie.
Il referente del Gruppo, se ritiene di poter risolvere il quesito in base alla propria conoscenza, fornirà la risposta al quesito posto, qualora la materia travalichi dalla propria professionalità, dovrà trasferire la questione al Gruppo, che con l'apporto multidisciplinare dei propri componenti valuterà la soluzione più opportuna.

La ***Tav. 10*** che segue riassume il sistema di relazioni sopra descritto:

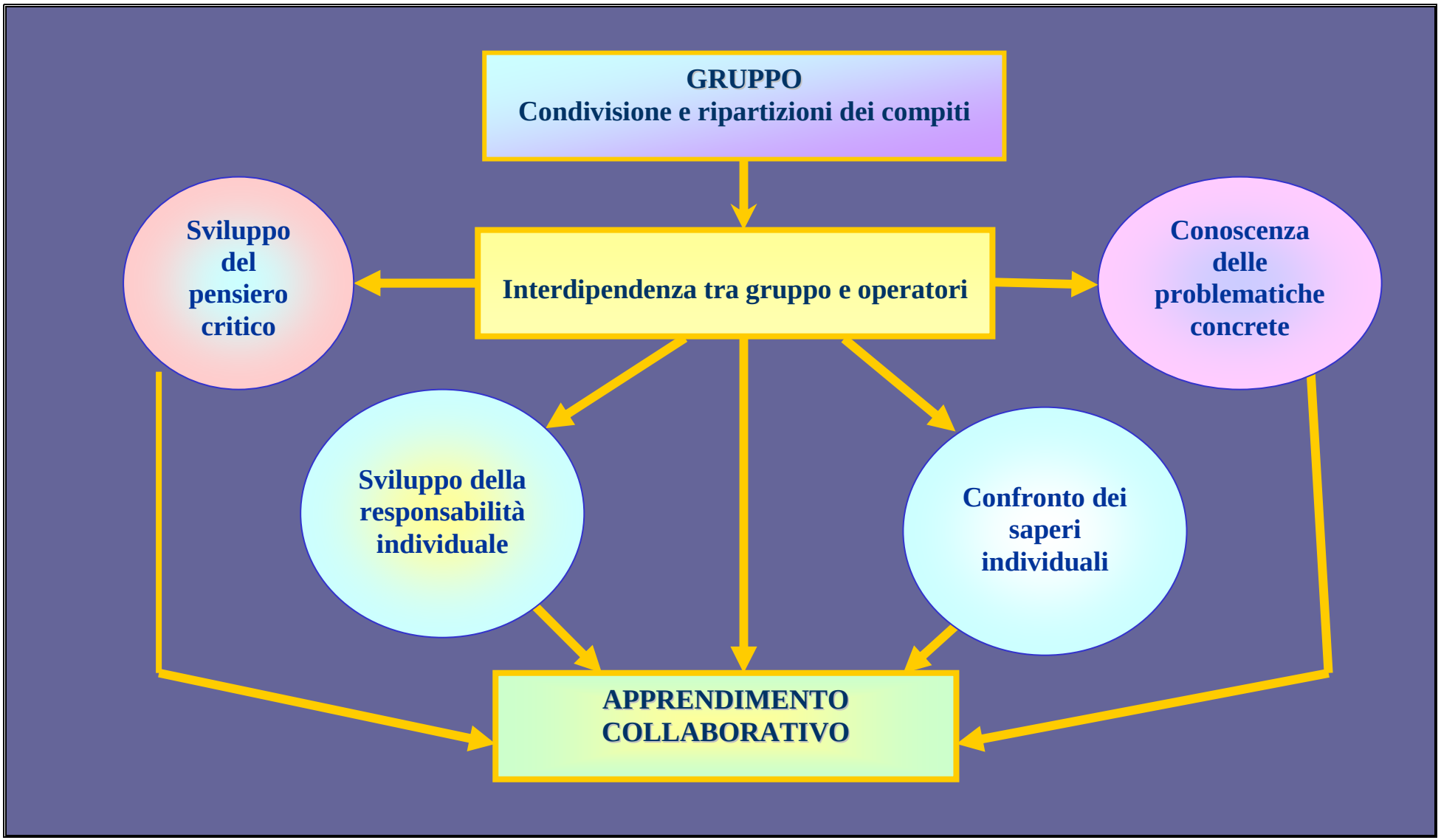
Tav. 10 – Sistema di relazioni



Inoltre, il Gruppo Privacy deve procedere all'attività di auditing, verificando la corrispondenza e la correttezza delle attività esercitate rispetto a quanto previsto in sede normativa.
La condivisione delle problematiche rappresenta lo strumento più idoneo a garantire la promozione della cultura sulla privacy, attuando uno scambio biunivoco tra il gruppo e gli operatori. Questi ultimi, infatti, sollevando al gruppo le concrete problematiche quotidiane ottengono la soddisfazione del proprio bisogno conoscitivo, e, nel contempo, trasmettono al gruppo la consapevolezza delle criticità che emergono nel contesto lavorativo.

La ***Tav. 11*** che segue offre una sintesi del concetto di *"apprendimento collaborativo"* sopra esposto.

Tav. 11 – Apprendimento collaborativo

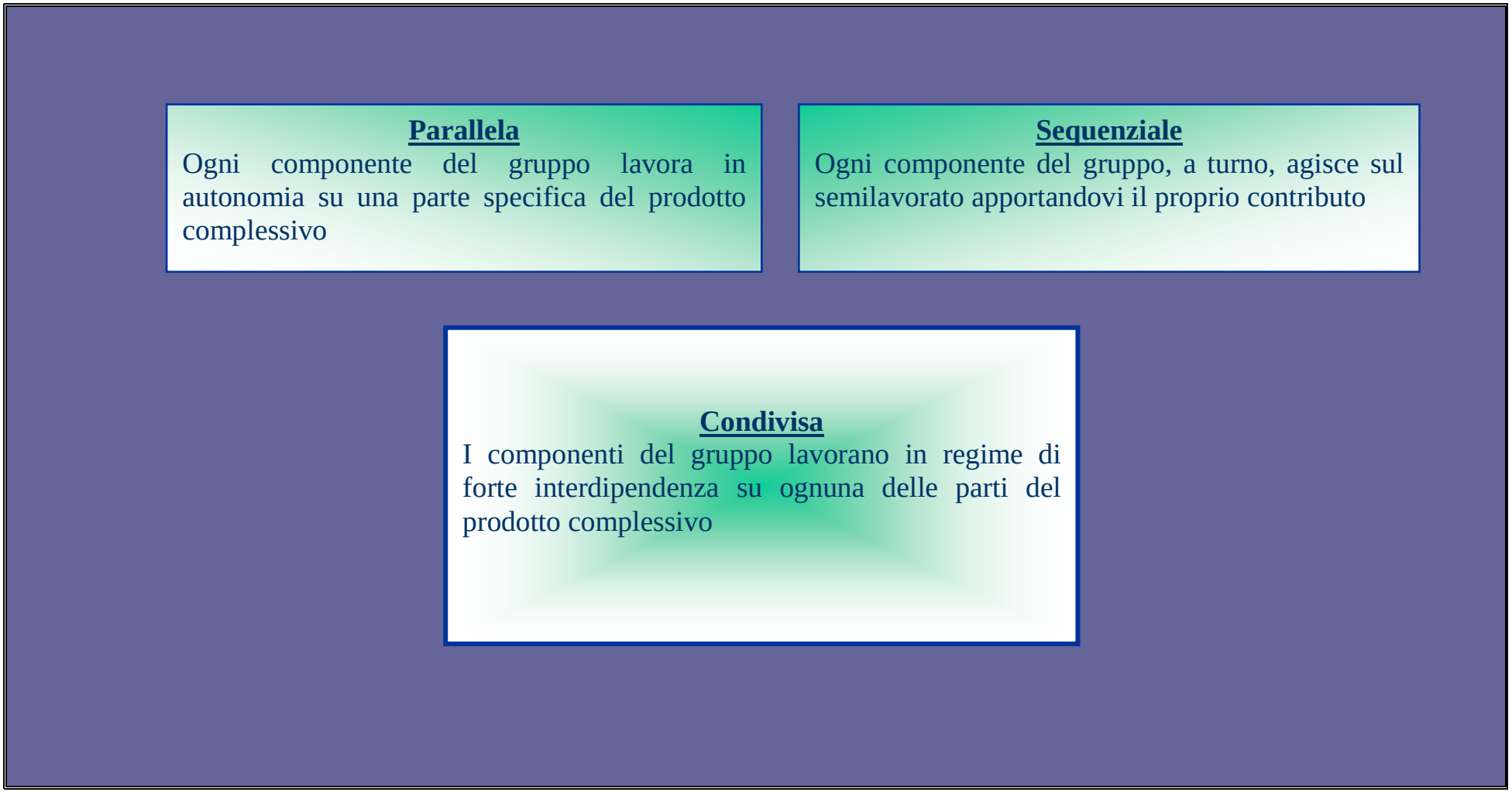


Il Gruppo Privacy si è dato una propria strategia organizzativa per operare le cui componenti sostanziali si possono così sintetizzare:

- ***Parallela***: ogni componente del gruppo lavora in autonomia su una parte specifica del prodotto complessivo.
- ***Sequenziale***: ogni componente del gruppo, a turno, agisce sul semilavorato apportandovi il proprio contributo.
- ***Condivisa***: i componenti del gruppo lavorano in regime di forte interdipendenza su ognuna delle parti del prodotto complessivo.

La ***Tav. 12*** che segue fotografa la strategia organizzativa sopra descritta:

Tav. 12 – Strategia organizzativa del Gruppo Privacy



Gli incaricati dovranno avere cura di instaurare un costante rapporto con il Gruppo ogni volta che inizia un nuovo progetto, una nuova attività, un nuovo trattamento o quanto quest'ultimo varia o cessa.
I rapporti che intercorrano tra gli incaricati delle strutture e il Gruppo Privacy dovranno essere intrattenuti relativamente a tutti gli obblighi da adempiere nei confronti del Garante (cfr. paragr. 2.2) e agli adempimenti rilevanti da porre in essere (cfr. paragr. 2.3), avendo riguardo a non omettere le informazione utile ad attuare le disposizioni del Codice, al fine di evitare di incorrere nel sistema delle sanzioni pecuniarie e penali previste.

La ***Tab. 10*** che segue riassume nel dettaglio, quali sono i rapporti che gli incaricati dovranno intrattenere con il Gruppo Privacy a fronte dei diversi adempimenti:

Tab. 10 – Sintesi dei rapporti tra gli incaricati e il Gruppo Privacy

Obblighi verso il Garante/Attività rilevanti	Rapporti con il gruppo
Inizio/variazione/cessazione nuovo trattamento	Gli incaricati sono tenuti a segnalare al Gruppo l'inizio ogni nuovo trattamento, la variazione, la cessazione del medesimo, ai fini di: ▪ valutare se sia opportuno procedere alla comunicazione al Garante; ▪ valutare e/o aggiornare notificazione; ▪ aggiornare il CE.TRA; ▪ mettere a punto nuove misure di sicurezza/aggiornare il DPS; ▪ nominare nuovi incaricati con assegnazione profilo e relativi ambiti di trattamento; ▪ aggiornamento anagrafe incaricati ▪ aggiornamento registri convenzioni /contratti/protocolli e registro comunicazione al Garante.
Autorizzazione	Nell'ambito delle segnalazioni attinenti agli altri adempimenti il Gruppo monitora l'evoluzione normativa circa l'autorizzazione, per ora non obbligatoria per ARS.
Notificazione	La notificazione deve essere sempre aggiornata, per non incorrere nelle sanzioni che il T.U. collega alla violazione delle disposizioni in materia. Perché ciò avvenga gli incaricati sono tenuti ad instaurare una forte interazione con il Gruppo Privacy, nel senso che gli stessi dovranno provvedere a segnalare tempestivamente l'inizio, la variazione o la cessazione di ogni trattamento per consentire al Gruppo di verificare se provvedere o meno a variare la notificazione al Garante.

Comunicazione	Gli incaricati sono tenuti a segnalare al Gruppo l'inizio/variazione di ogni trattamento, per consentire a questo ultimo di verificare se sia necessario effettuare la comunicazione al Garante e, in caso di risposta affermativa, il gruppo provvede a: ▪ trasmettere la comunicazione (o per via telematica con sottoscrizione digitale, o mediante telefax, o mediante lettera raccomandata, utilizzando il modello di comunicazione, predisposto dal Garante, che non ha ancora provveduto a predisporre; ▪ comunicare agli incaricati che i trattamenti possono iniziare non appena decorso il termine di 45 giorni dalla data di ricevimento della comunicazione da parte del Garante, salvo una diversa determinazione dello stesso, che può essere anche emessa ex post.
CE.TRA	Gli incaricati sono tenuti a comunicare tempestivamente al Gruppo l'inizio/variazione/cessazione di un trattamento, affinché quest'ultimo possa provvedere ad aggiornare il CE.TRA.
Misure di sicurezza/Documento Programmatico Sicurezza/	Gli incaricati sono tenuti a segnalare al Gruppo l'inizio/variazione/cessazione di ogni trattamento, per consentire a quest'ultimo di: ▪ mettere a punto le necessarie misure di sicurezza; ▪ verificare se sia necessario l'aggiornamento del documento programmatico della sicurezza.
Portale privacy	Gli incaricati sono tenuti a segnalare al Gruppo ogni variazione che intervenga sul trattamento dei dati agli stessi affidati, anche ai fini dell'aggiornamento delle informazioni contenute nel Portale Privacy.
Attività formativa	Gli incaricati sono tenuti a segnalare al Gruppo qualunque esigenza formativa utile ai fini dell'espletamento del proprio ruolo.

2.5.2 CE.TRA

L'ARS ha istituito[40] il censimento dei dati personali (CE.TRA.).
Il CE.TRA. contiene la rilevazione dei trattamenti dei dati suddivisi per tipologie e per strutture organizzative ed è tenuto a cura del Gruppo Privacy.
Il Gruppo provvede ad aggiornare il CE.TRA., qualora siano comunicati da parte del Titolare, dei Responsabili e degli incaricati del trattamento casi di attivazione di un

[40] Si veda in proposito la deliberazione CdA 28 giugno 2004, n. 18.

nuovo trattamento, variazioni rispetto ai trattamenti già presenti nel CE.TRA o cessazione di un trattamento in essere.
Il CE:TRA individua e cataloga:

- la descrizione dei dati sensibili trattati;
- la finalità e le modalità di trattamento;
- l'anagrafe dei Responsabili interni ed esterni e degli incaricati interni del trattamento di cui al successivo paragrafo 2.5.2.1;
- l'indicazione della banca dati cui il trattamento si riferisce;
- i luoghi di custodia;
- la tipologia dei supporti elettronici;
- l'individuazione tra i dati trattati con supporti elettronici o cartacei;
- la precisazione se i dati sono conservati in cassaforte.

Si veda ***Allegato 8*** relativo al CE.TRA. aggiornato a Gennaio 2008.

Per finalità di trasparenza, il CE.TRA sarà consultabile sul sito web del ARS "Portale Privacy".

2.5.2.1 Anagrafe responsabili/incaricati.

Il "Codice" per garantire l'effettivo esercizio dei diritti dell'interessato, impone al titolare del trattamento di adottare idonee misure volte, in particolare:

- ad agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi strumenti;
- a semplificare le modalità e a ridurre i tempi per il riscontro al richiedente.

Allo scopo di adempiere alle disposizioni del Codice l'Agenzia ha istituito, nell'ambito del CE:TRA, l'anagrafe dei Responsabili interni ed esterni e degli Incaricati al trattamento, onde agevolare e semplificare l'accesso alle informazioni che l'interessato può richiedere.
L'istituzione dell'Anagrafe dei Responsabili e degli Incaricati del trattamento" costituisce, altresì, una modalità operativa che consente di monitorare costantemente la situazione in essere, anche al fine di corrispondere ad ogni richiesta che possa pervenire dall'Ufficio del Garante o dalle autorità ispettive preposte (Guardia di Finanza).
In particolare il registro degli incaricati è utili anche ai fini della implementazione del sistema di autorizzazione degli accessi e della programmazione degli interventi formativi.

2.5.3 Registro delle autorizzazioni da richiedere al Garante/ Registro delle comunicazioni al Garante

L'istituzione dei Registri di cui al presente paragrafo, la cui tenuta e aggiornamento sono affidati al Gruppo Privacy, corrisponde all'esigenza di monitorare costantemente gli adempimenti a rilevanza esterna da attuare nei confronti del Garante in riferimento:

- ✓ ***all'obbligo di richiedere l'autorizzazione al Garante*** qualora ARS operi come organismo sanitario pubblico o in qualità di Ente pubblico per la comunicazione di dati sensibili o giudiziari al altro ente pubblico o privato, non prevista da specifica disposizione normativa e ove, in contemporanea, venissero meno l'autorizzazione generali concesse (si veda al riguardo quanto precisato al *paragr. 2.2.2);*
- ✓ ***all'obbligo di inviare la comunicazione al Garante*** (si veda al riguardo quanto precisato al *paragr. 2.2.3*) relativamente:
  - **al trattamento di dati idonei a rivelare lo stato di salute previsto dal programma di ricerca biomedica e/o sanitaria** (regolato dall'art. 12-*bis* del d.lgs. 502/1992), relativamente all'attività delle strutture scientifiche;
  - **alla comunicazione di dati personali (sensibili/giudiziari) da parte di ARS ad altro soggetto pubblico non prevista da norma di legge o di regolamento**, effettuata in qualunque forma anche mediante convenzione. Tale obbligo è riconducibile solo ad attività di competenza della struttura amministrativa.

Cfr Allegati 9 e 10.

2.5.4 Registro convenzioni/protocolli d'intesa/contratti affidamento trattamento dati a soggetti esterni. Registro convenzioni/protocolli d'intesa/contratti stipulati con altri enti ai fini dell'accesso da parte dell'ARS a flussi di dati attinenti alla salute ovunque collocati o per l'accesso da parte di altri enti ai dati di ARS

L'istituzione dei Registri di cui al presente paragrafo, la cui tenuta e aggiornamento sono affidati al Gruppo Privacy, corrisponde all'esigenza di monitorare costantemente l'evoluzione delle azioni da porre in essere in adempimento alle disposizioni del "Codice", con particolare riguardo all'osservanza degli obblighi nei confronti del Garante e degli adempimenti correlati alle attività rilevanti connesse ai trattamenti di dati sensibili.

Cfr Allegati 11 e 12.

2.5.5 La trasparenza in materia di Privacy – Il "Portale Privacy

Per favorire la più ampia trasparenza e correttezza nei confronti degli utenti e il pieno rispetto dei principi del Codice, in linea con il processo di innovazione della Pubblica amministrazione introdotto con la Circolare Funzione pubblica 13 marzo 2001, n. 3 "*Linee guida per l'organizzazione, l'usabilità e l'accessibilità dei siti web delle pubbliche amministrazioni*", l'ARS ha deciso di aprire uno specifico ***"Portale Privacy"*** con il duplice scopo di:

- consentire agli interessati ai trattamenti eseguiti da ARS di accedere liberamente e fruire di tutte le informazioni utili per l'esercizio dei propri diritti;
- promuovere la circolazione delle informazioni tra i soggetti che a vario titolo operano per perseguire il consolidamento della cultura della riservatezza, nel rispetto delle libertà fondamentali dell'individuo e della dignità della persona.

Il ***"Portale Privacy"*** sarà gestito ed implementato a cura del Gruppo Privacy e sarà organizzato come indicato nell'***Allegato 13.***:

CAPITOLO III

INCARICATI:

NOMINA, PROFILI DI AUTORIZZAZIONE
E
AMBITO DEL TRATTAMENTO CONSENTITO

ISTRUZIONI GENERALI E SPECIFICHE
PER GLI INCARICATI DELLE STRUTTURE ORGANIZZATIVE DI ARS

CAPITOLO III
INCARICATI: NOMINA, PROFILI DI AUTORIZZAZIONE E AMBITO DEL TRATTAMENTO CONSENTITO

Il presente capitolo affronta nello specifico il tema della figura dell'incaricato, delle modalità per la sua nomina, del "*profilo di autorizzazione*", assegnato a ciascun operatore, cioè dell'insieme di informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, i trattamenti ad essa consentiti, precisando le prescrizioni tecniche generali e specifiche che riguardano gli archivi gestiti con strumenti elettronici e cartacei, nonché le disposizioni relative alle comunicazioni elettroniche ed, infine, le istruzioni specifiche connesse a ciascun profilo di autorizzazione.

I paragrafi seguenti sono finalizzati a fornire le prescrizioni generali e specifiche agli incaricati, con lo sforzo di contestualizzare il più possibile le relative indicazioni. L'intento è quello di fornire un prodotto operativo e ampiamente fruibile per le singole strutture, attraverso il processo di applicazione della norma generale ed astratta alle dinamiche concrete di ogni singola struttura.

3.1 Nomina degli incaricati

L'incaricato è la persona fisica alla quale, nell'ambito delle proprie attività, il titolare o il responsabile affidano il trattamento dei dati personali (elaborazione, archiviazione, ecc.). L'incaricato è, dunque, colui che operativamente effettua i "trattamenti", attenendosi alle istruzioni del titolare o del responsabile

Il Codice, all'articolo 30, precisa che le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite. La designazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito. Si considera tale anche la documentata preposizione della persona fisica ad una unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima[41].

Le nuove disposizioni in materia di privacy attribuiscono agli incaricati un ruolo importante e delicato essendo questi i soggetti a cui è demandato il trattamento dei dati personali; dagli incaricati dipende, dunque, la correttezza e la liceità del trattamento nel rispetto dei principi della dignità della persona.

Con la deliberazione CdA n. 18 del 28 giugno 2004, come modificata dalle deliberazioni n. 5 del 13 aprile 2005 e n. 12 del 26 aprile 2007, sono stati individuati i profili da attribuire a ciascun incaricato, le relative funzioni, le operazioni eseguibili e le strutture/settori di appartenenza.

In particolare, si ponga mente alla seguente ***tabella 11***:

[41] Per ARS la nomina degli incaricati compete ai responsabili del trattamento secondo quanto disposto con deliberazione del CdA n. 18/2004 e ss.mm., con cui il titolare procede alla nomina dei Responsabili impartendo loro specifiche istruzioni.

Tab. 11 – Profili di autorizzazione

PROFILO/ DESCRIZIONE	STRUTTURA/ SETTORE	TIPOLOGIA DATI TRATTATI	OPERAZIONI ESEGUIBILI
A) AMMINISTRATORE BANCA DATI CENTRALE Responsabile della progettazione, del controllo e della manutenzione del database, delle sue prestazioni, dell'affidabilità e delle autorizzazioni all'accesso.	U.O. Centro Statistico Elaborazione Dati U.O. Tecnologie dell'Informazione	DATI COMUNI DATI SENSIBILI	1. Raccolta: • diretta presso l'interessato; • utilizzo di archivi regionali; • acquisizione archivi da soggetti terzi (pubblici o privati) 2. Registrazione 3. Organizzazione 4. Conservazione 5. Consultazione 6. Elaborazione 7. Modificazione 8. Selezione 9. Estrazione 10. Raffronto 11. Utilizzo 12. Interconnessione 13. Blocco 14. Comunicazione (su autorizzazione del Responsabile) 15. Diffusione (su autorizzazione del Responsabile) 16. Gestione della modalità di accesso 17. Cancellazione 18. Distruzione

Segue Tab. 11 - Profili di autorizzazione

PROFILO	STRUTTURA/ SETTORE	TIPOLOGIA DATI TRATTATI	OPERAZIONI
B) AMMINISTRA-TORE DI SISTEMA Gestisce il sistema operativo dell'elaboratore (Server o PC) che ospita il Database, eseguendo una serie di opera-zioni tecniche: dalla configura-zione generale al controllo dei diversi momenti di attività.	**U.O. Sistemi Informatici**	**DATI COMUNI** **DATI SENSIBILI**	**1. Raccolta** • **diretta presso l'interessato;** • **utilizzo di archivi regionali;** • **acquisizione archivi da soggetti terzi (pubblici o privati).** **2. Registrazione** **3. Organizzazione** **4. Conservazione** **5. Consultazione** **6. Elaborazione** **7. Modificazione** **8. Selezione** **9. Estrazione** **10. Raffronto** **11. Utilizzo** **12. Interconnessione** **13. Blocco** **14. Comunicazione (su autorizzazione Responsabile)** **15. Diffusione (su autorizzazione Responsabile)** **16. Gestione della modalità di accesso** **17. Cancellazione** **18. Distruzione**

Segue Tab. 11 – Profili di autorizzazione

PROFILO DESCRIZIONE	STRUTTURA/ SETTORE	TIPOLOGIA DATI TRATTATI	OPERAZIONI
C) AMMINISTRATORE BANCA DATI SPECIFICA *Detto profilo è attribuito per amministrare una banca dati specifica diversa da quella centrale* Responsabile della progettazione, del controllo e della gestione del database e delle sue prestazioni, dell'affidabilità e delle autorizzazioni all'accesso.	OSSERVATORI DIREZIONE: Area per lo studio e la ricerca del governo degli aspetti equitativi e la rilevanza economica dei bisogni sanitari U.O. Tecnologie dell'Informazione U.O. Centro Statistico Elaborazione Dati	DATI COMUNI DATI SENSIBILI	1. Raccolta • diretta presso l'interessato; • utilizzo di archivi regionali; • acquisizione archivi da soggetti terzi (pubblici o privati). 2. Registrazione 3. Organizzazione 4. Conservazione 5. Consultazione 6. Elaborazione 7. Modificazione 8. Selezione 9. Estrazione 10. Raffronto 11. Utilizzo 12. Interconnessione con altri dati 13. Blocco 14. Comunicazione (su autorizzazione del Responsabile) 15. Diffusione su (autorizzazione del Responsabile) 16. Gestione delle modalità di accesso 17. Cancellazione 18. Distruzione

Segue Tab. 11– Profili di autorizzazione

PROFILO	STRUTTURA/ SETTORE	TIPOLOGIA DATI TRATTATI	OPERAZIONI
D) UTENTE BANCA DATI CENTRALE *Detto profilo è attribuito agli utenti della banca dati centrale* Per mezzo di un linguaggio interattivo o tramite interfacce opportune, esegue applicazioni predefinite e interrogazioni sul database che non ne comportano la modifica, sia in termini di struttura che di contenuti	OSSERVATORI DIREZIONE: Area per lo studio e la ricerca del governo degli aspetti equitativi e la rilevanza economica dei bisogni sanitari	DATI COMUNI DATI SENSIBILI	1. Consultazione 2. Elaborazione 3. Selezione 4. Estrazione 5. Raffronto 6. Utilizzo 7. Interconnessione con altri archivi 8. Comunicazione (su autorizzazione del Responsabile) 9. Diffusione (su autorizzazione del Responsabile)
E) UTENTE BANCA DATI SPECIFICA Detto profilo è attribuito agli utenti di una banca dati specifica diversa dalla quella centrale	OSSERVATORI DIREZIONE: Area per lo studio e la ricerca del governo degli aspetti equitativi e la rilevanza economica dei bisogni sanitari U.O. Tecnologie dell'Informazione U.O. Centro Statistico Elaborazione Dati	DATI COMUNI DATI SENSIBILI	1. Consultazione 2. Elaborazione 3. Selezione 4. Estrazione 5. Raffronto 6. Utilizzo 7. Interconnessione con altri archivi 8. Comunicazione (autorizzazione Responsabile) 9. Diffusione (autorizzazione Responsabile)

Segue Tab. 11– Profili di autorizzazione

PROFILO	STRUTTURA/ SETTORE	TIPOLOGIA DATI	OPERAZIONI
F) AMMINISTRATORE BANCA DATI AMMINISTRATIVA *Questo profilo viene assegnato ai responsabili della gestione e manutenzione di dati informatizzati e cartacei contenenti dati sensibili e giudiziari inerenti la gestione del Personale e l'attività contrattuale della Direzione.* Responsabile della progettazione, del controllo e della gestione del database e delle sue prestazioni, dell'affidabilità e delle autorizzazioni all'accesso.	DIREZIONE: U.O. Personale e convenzioni Contabilità e bilancio U.O. Patrimonio, contratti e forniture	DATI SENSIBILI DATI GIUDIZIARI DATI COMUNI	1. Raccolta: • diretta presso l'interessato; • acquisizione archivi da altri soggetti esterni (pubblici o privati) 2. Registrazione 3. Organizzazione 4. Conservazione 5. consultazione 6. Elaborazione 7. Modificazione 8. Selezione 9. Estrazione 10. Raffronto 11. Utilizzo 12. Blocco 13. Comunicazione 14. Diffusione 15. Cancellazione 16. Distruzione
G) OPERATORE INSERIMENTO DATI Attraverso opportune interfacce, messe a disposizione dall'Amministratore banche dati, inserisce dati nel database	OSSERVATORI DIREZIONE	DATI SENSIBILI E GIUDIZIARI DATI COMUNI	1. Raccolta • Diretta presso l'interessato; • Utilizzo di archivi regionali; • Acquisizione archivi da soggetti terzi (pubblici o privati). 2. Registrazione 3. Consultazione

3.1.1. Assegnazione degli incarichi e comunicazione al Gruppo Privacy

I responsabili del trattamento nominano i loro collaboratori incaricati con ordine di servizio o determina, ***Allegato 14*** che dovrà essere compilato in ogni sua parte, con cui, tra l'altro, viene assegnato il profilo di autorizzazione.
Una copia di detto ordine di servizio o determina dovrà essere inviata all'incaricato del Gruppo Privacy per la manutenzione e gestione del CE.TRA (Censimento dei trattamenti) e per l'aggiornamento dell'anagrafe degli incaricati.
L'ordine di servizio o determina deve essere emanato ogni qualvolta:

1) viene creata una nuova banca dati che contenga dati sensibili o acquisito un nuovo flusso informativo di dati sensibili di cui ARS è titolare o co-titolare;
2) si debba assegnare, modificare o revocare un profilo di autorizzazione ad un incaricato.

L'ordine di servizio o determina deve contenere: l'ubicazione fisica della banca dati, una descrizione breve del contenuto, l'elenco degli utenti incaricati con il relativo profilo assegnato.
I dati raccolti dall'incaricato del Gruppo Privacy sono memorizzati nel CE.TRA sempre aggiornato per ottemperare agli obblighi di legge in materia.
Ai Coordinatori degli Osservatori nominati responsabili del trattamento con deliberazione del CdA n. 18/2004 e ss.mm., compete la nomina degli incaricati afferenti alle rispettive strutture scientifiche.
Al Direttore, nominato responsabile del trattamento con deliberazione del CdA n. 12/2007, compete la nomina degli incaricati della struttura tecnica amministrativa nonché di quelli assegnati ai settori/uffici trasversali che dipendendone funzionalmente dal Direttore medesimo.
Nei casi in cui il trattamento dei dati è effettuato, per alcune fasi, da strutture organizzative di ARS diverse, l'individuazione degli incaricati avviene con disposizione assunta d'intesa tra i Responsabili delle strutture interessate.
Gli incaricati hanno accesso ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati, nel rispetto del "*principio di necessità*" introdotto dal Codice[42]
L'atto con cui il Responsabile del trattamento individua gli incaricati non deve essere considerato come mero adempimento cui assolvere *una tantum*, bensì comporta l'impegno collettivo ad un aggiornamento delle prescrizioni, coerente con i mutamenti organizzativi e di assegnazione degli incarichi al personale.
La conoscenza dei dati personali da parte di chi sia stato nominato incaricato non è considerata "comunicazione".

In sede di prima applicazione delle presente disposizioni, la nomina degli incaricati, i relativi profili di autorizzazione e l'ambito del trattamento consentito sono individuati *nell'allegato sub lettera "A"* alla determina del responsabile, in base alla ricognizione

[42] Una novità introdotta è il "***principio di necessità***" del trattamento dei dati (art. 3 del Codice). Esso afferma che i sistemi informativi ed i programmi informatici devono essere configurati riducendo al minimo l'uso dei dati personali/dati identificativi. Così il loro trattamento è escluso quando le finalità perseguite nei singoli casi possono essere realizzate mediante dati anonimi o opportune modalità che permettono di identificare l'interessato solo in caso di necessità. Il nuovo principio integra e completa il principio di ***pertinenza*** e ***non eccedenza*** dei dati trattati, in base ai quali i dati possono essere trattati solo se funzionali al raggiungimento degli scopo legittimi perseguiti, completi e non eccessivi rispetto agli scopo stessi.

generale dei trattamenti effettuata sia in relazione alla notificazione al Garante, sia in sede di istituzione e aggiornamento del CE.TRA.

3.2. Istruzioni generali per gli incaricati

3.2.1. Trattamento dei dati personali

Gli incaricati devono eseguire i trattamenti secondo le disposizioni contemplate nel presente documento.
Gli incaricati hanno accesso ai soli dati personali la cui conoscenza sia strettamente necessaria al trattamento.

In particolare, gli incaricati dovranno avere cura che i dati personali siano:

- trattati in modo lecito e secondo correttezza;
- raccolti e registrati per scopi determinati, espliciti e legittimi ed in funzione delle svolgimento dei compiti istituzionali, nei limiti stabiliti dal Codice;
- necessari;
- esatti e, se necessario, aggiornati;
- pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono stati raccolti;
- conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali sono stati raccolti o successivamente trattati;
- nel pieno rispetto delle misure minime di sicurezza, custodendo e controllando i dati oggetto di trattamento in modo da evitare i rischi, anche accidentali, di distruzione o perdita, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta. Le misure minime di sicurezza (di cui agli artt. 33 – 36 ed allegato B del citato Codice privacy) sono obbligatorie e sono distinte in funzione delle seguenti modalità di trattamento dei dati:
  - ✓ senza l'ausilio di strumenti elettronici (es. dati in archivi cartacei o su supporto magnetico/ottico);
  - ✓ con strumenti elettronici (PC ed elaboratori).

Tali requisiti valgono anche per le copie di scarto dei documenti che sono equiparati ai documenti stessi.
Ai fini della sicurezza dei dati personali, qualunque prodotto dell'elaborazione degli stessi, ancorché non costituente documento definitivo (appunti, stampe interrotte, stampe di prova, elaborazioni temporanee etc.), va trattato con le stesse cautele riservate alla versione definitiva. Pertanto tali materiali, quando non più utili, devono essere sistematicamente distrutti e la loro distruzione deve avvenire in modo controllato e con modalità tale da assicurare il non utilizzo dei dati.
A tale scopo il Settore competente fornisce alle strutture operative di ARS lo strumento (macchina distruggi - documenti), per eliminare le copie di scarto, in numero sufficiente alle esigenze ed in modo tale da garantire che le informazioni contenute non siano tecnicamente ricostruibili in alcun modo e non siano accessibili ad altri soggetti non autorizzati al trattamento.
Attualmente la distruzione dei documenti non più validi, segue le regole imposte dalle legge archivistica del 1963 e dal Codice unico dei beni culturali del 2004 sulle copie di scarto.

Il Gruppo Privacy dovrà porre particolare attenzione alla progettazione, realizzazione e aggiornamento dei Sistemi Informativi i quali, nel rispetto del principio di necessità (art. 3 Codice), devono essere configurati in modo tale da ridurre al minimo l'utilizzazione di dati personali ed identificativi.
E' necessario infatti evitare il trattamento dei dati sensibili ed identificativi quando le finalità perseguite nei singoli casi possono essere realizzate mediante dati anonimi, limitando l'identificazione dell'interessato solo ai casi di effettiva necessità.

3.2.2. Cifratura o separazione degli altri dati personali dell'interessato

Gli incaricati dovranno attenersi alle seguenti istruzioni in materia di cifratura o separazione degli altri dati personali dell'interessato.
Secondo quanto previsto dal Codice (art. 22 e 34) i dati idonei a rilevare lo stato di salute e la vita sessuale devono essere conservati separatamente da ogni altro dato personale trattato per finalità che non richiedono il loro utilizzo.
I dati sensibili o concernenti i provvedimenti giudiziari contenuti in elenchi, registri, banche di dati, tenuti con l'ausilio di mezzi elettronici o comunque automatizzati, nonché i dati idonei a rilevare lo stato di salute e la vita sessuale, indipendentemente dalle modalità di trattamento, *devono essere trattati con tecniche di cifratura o mediante l'utilizzo di codici identificativi* o di altri sistemi, che considerato il numero e la natura dei dati trattati, permettono di identificare gli interessati solo in caso di effettiva necessità.
L'adozione di tecniche di **separazione dei dati sensibili e giudiziari dai dati identificativi** investe aspetti progettuali del database e quindi risulta preferibile laddove si stia creando un nuovo trattamento dati con relativo database oppure quando i costi in termini di risorse umane ed economiche per l'adozione di tale tecnica siano accettabili.
Nel caso di questa tipologia di dati bisogna comunque mantenere la privatezza degli stessi quando questi, eventualmente correlati tra di loro, vengono trasferiti tra il sistema centrale ed il client sul quale l'incaricato opera.
I dati personali sensibili o concernenti provvedimenti giudiziari non possono essere trattati nell'ambito di test psicoattitudinali volti a definire il profilo e la personalità dell'interessato.
Le operazioni *di raffronto tra dati sensibili e/o dati concernenti provvedimenti giudiziari* possono essere effettuate solo con 'indicazione scritta dei motivi. Se tali operazioni sono svolte utilizzando banche dati di diversi titolari, sono ammesse solo se previste da espressa disposizione di legge (art. 22, comma 10 e 11 Codice).

Per la diffusione di dati personali sensibili tramite pubblicazione sul BURT si fa espresso riferimento a quanto precisato al § *2.3.6.1.*

3.2.3 Trattamento di dati personali giudiziari

Si tratta di dati idonei a rilevare provvedimenti in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti (art. 3, comma 1, lett, da a) a o) e da r) a u) del d.p.r. 14 novembre 2002, n. 313) oppure la qualità di imputato o di indagato (artt. 60 e 61 Codice di procedura penale).

Tali dati riguardano:

a) i provvedimenti giudiziali penali di condanna definitivi, anche pronunciate da autorità giudiziarie straniere se riconosciute ai sensi degli articoli 730 del Codice di procedura penale, salvo quelli concernenti contravvenzioni per le quali la legge ammette la definizione in via amministrativa o l'oblazione limitatamente alle ipotesi di cui all'articolo 162 del Codice penale, sempre che per quelli esclusi non sia stata concessa la sospensione condizionale della pena;
b) i provvedimenti giudiziari definitivi concernenti le pene, compresa la sospensione condizionale e la non menzione, le misure di sicurezza personali e patrimoniali, gli effetti penali della condanna, l'amnistia, l'indulto, la grazia, la dichiarazione di abitualità, di professionalità nel reato, di tendenza a *delinquere*;
c) i provvedimenti giudiziari concernenti le pene accessorie;
d) i provvedimenti giudiziari concernenti le misure alternative alla detenzione;
e) i provvedimenti giudiziari concernenti la liberazione condizionale;
f) i provvedimenti giudiziari definitivi che hanno prosciolto l'imputato o il non luogo a procedere per difetto di imputabilità, o disposto una misura di sicurezza;
g) i provvedimenti giudiziari definitivi di condanna alle sanzioni e i provvedimenti di conversione di cui all'articolo 66, terzo comma e all'articolo 108, terzo comma, della legge 24 novembre 1981, n. 689;
h) i provvedimenti giudiziari del pubblico ministero previsti dall'articolo 656, comma 5, 657 e 663 del Codice di procedura penale;
i) i provvedimenti giudiziari di conversine delle pene pecuniarie;
j) i provvedimenti giudiziari definitivi concernenti le misure di prevenzione della sorveglianza speciale semplice o con divieto o obbligo di soggiorno;
k) i provvedimenti giudiziari concernenti la riabilitazione;
l) i provvedimenti giudiziari di riabilitazione di cui all'articolo 15 della legge 3 agosto 1988, n. 327;
m) i provvedimenti giudiziari di riabilitazione speciale relativi ai minori, di cui all'art. 24 della legge 27 maggio 1935, n,. 835;
n) i provvedimenti giudiziari relativi all'espulsione a titolo di sanzione sostitutiva o alternativa alla detenzione, ai sensi dell'articolo 16 del decreto legislativo 25 luglio 1998, n. 286, come sostituito dall'articolo 15 della legge 30 luglio 2002, n. 189;
o) i provvedimenti amministrativi di espulsione ed i provvedimenti giudiziari che decidono il ricorso avverso i primi, ai sensi dell'articolo 13 del decreto legislativo 25 luglio 1998, n. 286, come modificato dall'articolo 12 della legge 30 luglio 2002, n. 189;
p) i provvedimenti di correzione, a norma di legge, dei provvedimenti già iscritti;
q) qualsiasi altro provvedimento che concerne a norma di legge i provvedimenti già iscritti, come individuato con decreto Presidente della Repubblica, ai sensi dell'articolo 17, comma 1, della legge 23 agosto 1988, n. 400, su proposta del Ministro della giustizia.

Il trattamento dei dati giudiziari – compresa la loro comunicazione - è ammesso solo se autorizzato da espressa disposizione di legge o provvedimento del Garante che specifichi le rilevanti finalità di interesse pubblico del trattamento stesso, i tipi di dati trattati e le precise operazioni autorizzate.

In relazione alle rilevanti finalità di interesse pubblico individuate dal d.lgs. 196/2003, i soggetti pubblici devono identificare e rendere pubblici, anche i tipi di

dati e le operazioni oggetto del trattamento concernenti dati giudiziari (artt. 21 e 22 Codice).
La diffusione dei dati giudiziari, così come quella dei dati sensibili, è ammessa solo se prevista da espressa disposizione di legge.

Per la diffusione di dati giudiziari tramite pubblicazione sul BURT si fa espresso riferimento a quanto precisato al § *2.3.6.2.*

3.2.4 Ulteriori prescrizioni

Gli incaricati sono tenuti inoltre a:

- segnalare al Gruppo Privacy, secondo quanto indicato al *paragrafo 2.5.1:*
  - eventuali circostanze che rendano necessario od opportuno l'aggiornamento delle predette misure di sicurezza (DPS) al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, ai fini dell'aggiornamento del C.E.T.R.A.;
  - la necessità della comunicazione e della diffusione dei dati esclusivamente ai soggetti indicati dal titolare o dal responsabile, secondo le modalità fissate dall'art. 35 del Regolamento generale di organizzazione dell'ARS approvato con deliberazione della Giunta regionale 21.01.08, n. 29;
- mantenere, salvo quanto precisato al punto precedente, la massima riservatezza sui dati personali dei quali si venga a conoscenza nello svolgimento dell'incarico, per tutta la durata del medesimo ed anche successivamente al termine di esso;
- svolgere, in ogni caso, il trattamento dei dati personali per le finalità e secondo le modalità stabilite, anche in futuro, dal titolare e dal responsabile e, comunque, in modo lecito e secondo correttezza;
- fornire al responsabile, a semplice richiesta e secondo le modalità indicate da questi, tutte le informazioni relative all'attività svolta, al fine di consentire loro di svolgere efficacemente la propria attività di controllo;
- in generale:
  - prestare la più ampia e completa collaborazione con il responsabile al fine di compiere tutto quanto sia necessario ed opportuno per il corretto espletamento dell'incarico nel rispetto della normativa vigente;
  - relazionarsi costantemente con il Gruppo Privacy;
- verificare che i dati trattati siano pertinenti, completi e non eccedenti le finalità per le quali sono stati raccolti o successivamente trattati;
- è vietato creare nuove banche dati o copiare banche dati già esistenti senza espressa autorizzazione del responsabile del trattamento;
- è vietato trasmettere a mezzo e-mail dati sensibili (anche adottando tecniche di compressione con password); qualora si renda necessario, previa autorizzazione del responsabile, una trasmissione di dati sensibili occorre rivolgersi all'amministratore di sistema che adotterà le misure precauzionali necessarie al compimento dell'operazione;
- mantenere assoluto riserbo sui dati personali e/o sensibili di cui si viene a conoscenza nell'esercizio delle proprie funzioni;
- è vietato asportare supporti informatici o cartacei contenenti dati personali e/o sensibili senza la previa autorizzazione del responsabile del trattamento;

- i supporti informatici o cartacei contenenti dati personali e/o sensibili devono essere conservati negli appositi armadi o casseforti ignifughe;
- le password di accesso alle banche dati sono personali e non cedibili a nessuno e per nessun motivo; qualora si sospetti che la propria password abbia perso la caratteristica di segretezza è necessario procedere con l'immediata sostituzione; la password non deve essere trascritta in nessun luogo *(cfr. paragr. 3.2.6);*
- in caso di allontanamento dal posto di lavoro, anche momentaneo, per evitare l'accesso ai dati da parte di terzi non autorizzati, deve essere bloccato il computer; nello specifico dei sistemi Windows; tale operazione avviene premendo contemporaneamente ctrl-alt-canc e cliccando sul pulsante "blocca computer" *(cfr. paragr. 3.2.6)*..

La Tabella 10, ***paragr. 2.5.1,*** riassume i principali obblighi degli incaricati nei confronti del Gruppo Privacy

3.2.5 Linee guida per gli incaricati in merito alle misure minime di sicurezza

Oltre alle prescrizioni già fornite al § *2.3.2. "Documento programmatico sulla Sicurezza"*
Gli incaricati dovranno attenersi alle seguenti disposizioni in materia di misure minime di sicurezza:

1. **Utilizzate le chiavi**
   Il primo livello di protezione di ciascun sistema è quello fisico; è vero che un armadio chiuso a chiave può in molti casi non costituire una protezione non sufficiente ma pone se non altro un primo ostacolo e richiede comunque uno sforzo volontario e non banale per aprirlo. Quando gli incaricati si allontano dal proprio ufficio devono chiudere i documenti a chiave nei cassetti e/o armadi.
2. **Conservate i supporti estraibili (floppy disk, cd-rom chiavi usb, etc.) in luogo sicuro**
   Per i supporti estraibili si applicano gli stessi criteri che per i documenti cartacei, con l'ulteriore pericolo che il loro smarrimento (che può essere anche dovuto ad un furto) può passare facilmente inosservato. A meno che gli incaricati non siano sicuri che non contengano dati personali, gli stessi devono essere riposti sotto chiave non appena finito di usarli.
3. **Utilizzate le password**
   Vi sono varie categorie di password, ognuno con il proprio ruolo preciso.
   - ✓ La password di accesso al computer impedisce l'utilizzo improprio della postazione quando, per qualsiasi motivo, l'incaricato non si trova in ufficio.
   - ✓ La password di accesso alla rete impedisce che l'eventuale accesso non autorizzato ad una postazione renda disponibili tutte le risorse dell'Ufficio.
   - ✓ La password di programmi specifici permette di restringere l'accesso ai dati al solo personale autorizzato.
   - ✓ La password del salva schermo, infine, impedisce che l'assenza temporanea dell'incaricato permetta ad una persona non autorizzata di accedere alle risorse del suo computer.

4. **Come deve essere scelta la password**
   La paralo chiave per l'accesso al sistema deve essere composta da almeno otto caratteri e nel caso che il sistema non lo permetta dal numero massimo consentito. La parola chiave non deve contenere caratteri riconducibili all'incaricato ed è modificata al primo utilizzo e successivamente ogni tre mesi.
5. **Non fatevi spiare quando state digitando la password**
   Occorre evitare che al momento in cui gli incaricati digitano la loro password qualcuno possa scrutare la battitura, anche se sussistono buone capacità di dattiloscrittura.
6. **Custodite la password in luogo sicuro**
   Occorre evitare di scrivere la propria password, meno che mai vicino alla postazione di lavoro. L'unico affidabile dispositivo di registrazione è la memoria. Se sussiste la necessità di conservare traccia della password per iscritto, occorre non lasciare in giro i fogli utilizzati.
7. **Per evitare l'identificazione della password**
   - ✓ NON bisogna comunicare a nessuna la propria: occorre ricordare che lo scopo per cui viene usata una password è assicurare che nessun altro possa utilizzare le risorse dell'incaricato e farlo a suo nome.
   - ✓ NON bisogno scegliere password contenute in dizionari. Su alcuni sistemi è possibile "provare" tutte le password contenute nel dizionario per vedere quale sia quella giusta.
   - ✓ NON si deve credere che usare parole straniere renda difficile il lavoro di scoperta; infatti chi vuole scoprire una password è dotato di molti dizionari di svariate lingue.
   - ✓ E' vietato usare il proprio nome utente. E' la password più facile da indovinare.
   - ✓ NON bisogna usare password collegate in qualche modo all'incaricato come ad es., il proprio nome, quello della moglie/marito, dei figli, del cane, date di nascita, numeri di telefono, etc.
8. **Attenzione alle stampe di documenti riservati**
   Non bisogna lasciare accedere alle stampe persone non autorizzate; se la stampante non si trova nell'ufficio occorre che l'incaricato si rechi con rapidità a ritirare le stampe. L'incaricato deve distruggere personalmente le stampe non più utili.
9. **Non lasciate traccia dei dati riservati**
   Quando viene rimosso un file, i dati non vengono effettivamente cancellati ma soltanto marcati come non utilizzabili, ma sono facilmente recuperabili. Neanche la formattazione assicura la loro eliminazione; solo l'utilizzo di un programma apposito garantisce che sul dischetto non resti traccia dei dati precedenti. Nel dubbio è meglio usare un dischetto, o altro supporto estraibile, nuovo.
10. **Prestate attenzione all'utilizzo dei PC portatili**
    I PC portatili sono un facile bersaglio per i ladri. Se gli incaricati hanno necessità di gestire dati riservati su portatile, occorre farsi installare un buon programma di cifratura del disco rigido ed utilizzare una procedura di backup periodico.
11. **Non fate usare il vostro computer a personale esterno a meno di non essere sicuri della loro identità**

Personale esterno può avere bisogno di installare un nuovo sofware/hardware nel computer dell'incaricato. Occorre assicurarsi dell'identità della persona e dell'autorizzazione ad operare sul proprio computer.

12. **Non utilizzate apparecchi non utilizzati**
    L'utilizzo di modem o postazioni di lavoro collegate in rete offre una porta d'accesso dall'esterno non solo ai singoli computer ma a tutta la Rete ed è quindi vietato. Per utilizzo di altri apparecchi occorre consultarsi con il responsabile informatico del Gruppo Privacy.
13. **Non installate programmi non autorizzati**
    Solo i programmi istituzionali e acquistati dall'Amministrazione con regolare licenza sono autorizzati. Se il lavoro degli incaricati richiede l'utilizzo di programmi specifici, occorre consultarsi con il responsabile informatico del Gruppo Privacy.
14. **Per garantire il ripristino dei dati fate dei backup periodici**
    I dati potrebbero essere gestiti da un *file server*, oppure essere gestiti in locale e trasferiti in un server solo al momento del backup, oppure salvati su supporto removibile (cd-rom, floppy-disk, chiavi usb, etc).
15. **Applicate con cura le seguenti linee guida per la prevenzione da infezione da virus**
    La prevenzione delle infezioni da virus sul proprio computer è più facile e comporta uno spreco di risorse minori della correzione degli effetti di un virus; il pericolo è di incorrere in una perdita irreparabile dei dati.
    Che cos'è un virus:
    Il virus è un programma in grado di trasmettersi autonomamente e che può causare effetti dannosi. Alcuni virus si limitano a riprodursi senza ulteriori effetti. Altri si limitano alla semplice visualizzazione di messaggio sul video, i più dannosi arrivano a distruggere tutto il contenuto del disco rigido.
    Come si trasmette un virus:
    - ✓ attraverso programmi;
    - ✓ attraverso le macro dei programmi di automazione d'ufficio.

    Come NON si trasmette un virus:
    - ✓ attraverso file di dati non in grado di contenere macro (file di testo, html, pdf, etc.);
    - ✓ attraverso mail non contenenti allegati.

    Quando il rischio da virus si fa serio:
    - ✓ quando si installano i programmi;
    - ✓ quando si copiano dati da dischetti;
    - ✓ quando si scaricano dati o programma da Internet.

    Alcuni effetti provocati da virus:
    - ✓ effetti sonori e messaggi sconosciuti appaiono sul video;
    - ✓ nei menù appaiono funzioni extra finora non disponibili;
    - ✓ lo spazio disco residuo si riduce inspiegabilmente.

    Come prevenire i virus:
    1. **Usate soltanto programmi provenienti da fonti fidate**
       Copie sospette di programmi possono contenere virus o altro sofware dannoso.
       Ogni programma deve essere sottoposto alla scansione prima di essere installato.

Non utilizzate programmi non autorizzati, con particolare riferimento ai videogiochi, spesso utilizzati per veicolare virus.

2. **Assicuratevi di non far partire accidentalmente il vostro computer da dischetto**
   Se il dischetto o altro supporto fosse infettato il virus si trasferirebbe nella memoria potrebbe spandersi agli altri files.
3. **Proteggete i vostri dischetti da scrittura o altri supporti quando possibile**
   In questo modo eviterete le scritture accidentali, magari tentate da un virus che tende a propagarsi. I virus non possono in ogni caso aggirare la protezione meccanica.
4. **Assicuratevi che il vostro software antivirus sia aggiornato**
   La tempestività dell'azione di bonifica è essenziale per limitare i danni che un virus può causare; inoltre è vitale che il programma antivirus conosca gli ultimi aggiornamenti sulle "impronte digitali" dei nuovi virus.
5. **Non diffondete messaggi di provenienza dubbia**
   Se ricevete messaggi che avvisano di un nuovo virus pericolosissimo, ignorateli: le e-mail di questo tipo sono dette con terminologia anglosassone *hoax* (termine tradotto spesso in italiano con "bufala"). Questo è vero anche se il messaggio arriva dal vostro migliore amico, dal vostro capo, da un vostro parente o da un tecnico informatico. E' vero anche se si fa riferimento ad "una notizia proveniente dalla Microsoft" oppure "dall'IBM" (sono gli *hoax* più diffusi).
6. **Non partecipate a catene di "S. Antonio" e simili**
   Analogamente, tutti i messaggi che vi invitano "a diffondere la notizia quanto più possibile" sono *hoax,* anche se parlano della fame nel mondo, della situazione delle donne negli stati arabi, di una bambina in fin di vita, se promettono guadagni miracolosi o grande fortuna; sono tutti *hoax* aventi molto spesso scopi molto simili a quelli dei virus, cioè utilizzare indebitamente le risorse informatiche.

3.2.5.1 Sicurezza degli archivi cartacei

Anche per i dati personali trattati manualmente devono essere adottate adeguate misure di sicurezza.
Gli archivi cartacei si distinguono in:

- ✓ archivi di lavoro mantenuti a cura dei singoli incaricati;
- ✓ archivio dei fascicoli del personale: archivio ufficiale mantenuto a cura di un incaricato in locale riservato;
- ✓ archivio generale di deposito: archivio mantenuto per esigenze di legge, mantenuto a cura di uno o più incaricati in locali di sicurezza o in armadi provvisti di serratura.

3.2.5.1.1 Archivi di lavoro

Il personale incaricato del trattamento opera rispettando le seguenti istruzioni:

- ✓ gli armadi o altre strutture di conservazione devono essere chiusi a chiave;
- ✓ nel corso del trattamento, i documenti sono conservati in appositi contenitori di lavoro chiusi, specie durante la pausa di lavoro o quando il personale incaricato deve assentarsi dal posto di lavoro o dall'ufficio;
- ✓ eventuali fotocopie devono essere custodite con le stesse modalità dei documenti originali. La loro distruzione deve avvenire con le modalità individuate nel *§ 3.2.2.*

3.2.5.1.2 Archivio dei fascicoli del personale

Nell'accedere ai documenti cartacei l'incaricato deve seguire le seguenti prescrizioni:

- ✓ gli armadi o altre strutture di conservazione sono tenuti chiusi a chiave;
- ✓ i documenti, chiusi in appositi contenitori di lavoro sono custoditi in un locale apposito; il locale è presieduto dal personale incaricato, che durante le pause di lavoro o durante l'assenza dall'ufficio, ha l'obbligo di chiuderlo a chiave;
- ✓ i documenti sono prelevati dagli archivi per il tempo strettamente necessario allo svolgimento della mansione;
- ✓ eventuali fotocopie devono essere custodite con le stesse modalità dei documenti originali.

3.2.5.1.3 Archivio storico

L'archivio generale risiede in un locale apposito chiuso a chiave e in armadi provvisti di serratura.

L'accesso a tale archivio è consentito esclusivamente agli incaricati specificatamente autorizzati con ordine di servizio.

Istruzioni specifiche per gli incaricati degli Osservatori di Epidemiologia, per la Qualità e per gli incaricati dei settori/uffici con funzioni trasversali assegnati funzionalmente alla Direzione

Il paragrafo affronta nello specifico le istruzioni da impartire agli incaricati del trattamento delle strutture scientifiche e dei settori ed uffici cui sono assegnate funzioni a carattere trasversale, assegnati funzionalmente alla Direzione, con modalità strettamente correlata ai profili di autorizzazione

3.3.1 Profili e relative istruzioni

La metodologia di lavoro adottata e le disposizioni a cui attenersi sono funzione del profilo assegnato all'incaricato:

3.3.1.1 Amministratore banca dati centrale A

Questo profilo viene assegnato agli sviluppatori delle banche dati denominate "Centrali".
La banche dati centrali risiedono sui Server di ARS.
Al momento i Server in uso sono:

- Archimede
- Webserver
- Server Intranet.

E' compito di questo profilo gestire e sviluppare le banche dati in oggetto adottando idonee tecniche informatiche nel rispetto della normativa Privacy.
Gli incaricati a cui è assegnato questo profilo dovranno attenersi alle seguenti istruzioni specifiche in relazione alle operazioni di seguito identificate:

- *Separazione e Cifratura*

La banca dati si compone di più archivi che devono essere organizzati in modo tale da garantire la separazione tra i dati personali e i dati sensibili, l'interconnessione tra le due tipologie di dati può avvenire solo per mezzo di questo profilo che è in possesso della password di amministrazione del Database.

L'interconnessione tra dati personali e dati sensibili viene resa disponibile anche agli incaricati di profilo D solo per il tempo necessario al trattamento, dopo esplicita richiesta a mezzo e-mail agli amministratori con profilo A che hanno il compito di regolarne l'accesso e di chiuderlo a fine trattamento.

Ai fini dell'analisi statistica sui soggetti, le tabelle dati contenenti le sole informazioni sulla salute possono includere degli identificativi personali generati per mezzo di algoritmi di cifratura a chiave segreta a partire dai dati personali.
E' compito di questo profilo cifrare i dati suddetti e custodire la chiave segreta di decriptazione.

- *Gestione profili accesso degli incaricati*

E' compito degli incaricati di questo profilo gestire e monitorare tutti gli accessi degli incaricati del profilo D alla banca dati centrale regolandone e attivandone le policy sui singoli archivi in base agli incarichi loro assegnati.

- *Conservazione dei supporti originali e password*

In qualità di amministratori, gli incaricati di questo profilo provvedono all'aggiornamento della banca dati.
I supporti informatici su cui sono memorizzati i dati originali provenienti da enti esterni ad ARS (per la quasi totalità si tratta di dati provenienti dalla Regione Toscana) al termine di ogni trattamento (accodamento alla banca dati centrale) devono essere riposti e custoditi presso l'apposita cassaforte ignifuga situata in V.le Milton in "Aula Etnica".
Una copia della password di amministrazione dovrà essere anch'essa custodita nella suddetta cassaforte.

- *accesso alla cassaforte ignifuga*

L'accesso alla cassaforte avviene per mezzo di una password custodita dagli incaricati del profilo A e B;

3.3.1.2 Amministratore di sistema B

A questo profilo compete la gestione dell'infrastruttura informatica dell'ARS.

In particolare è compito di questo profilo:
- gestire le autenticazioni e le modalità di accesso alla rete;
- gestire i DataBase Management System;
- attuare l'accesso al sistema di trasferimento di dati on-line dalla Regione Toscana;
- gestire i backup e la conservazione delle banche dati;
- gestire e mantenere le cartelle crittografate;
- supportare le operazioni di trattamento.

3.3.1.3 Amministratore banca dati specifica C

Questo profilo viene assegnato agli sviluppatori e/o responsabili della gestione e manutenzione di banche dati contenenti dati sensibili e che non fanno parte della banca dati Centrale.
Gli incaricati a cui è assegnato questo profilo dovranno attenersi alle seguenti istruzioni specifiche in relazione alle operazioni di seguito identificate:

- *gestione profili accesso degli incaricati*

E' compito degli incaricati di questo profilo gestire e monitorare tutti gli accessi degli incaricati del profilo "E" alla banca dati regolandone e attivandone i permessi.

Le banche dati specifiche devono essere sviluppate con strumenti adeguati a garantire agevolmente le misure di sicurezza. Gli archivi che non sono sviluppati nella banca dati centrale devono essere implementati con motori di database adeguati.
La scelta del software per lo sviluppo delle maschere di inserimento dati o di interfaccia al Database è libera, mentre la struttura e le tabelle che contengono fisicamente i dati devono essere gestite da un motore database adatto a garantire la gestione dei profili d'accesso, la separazione tra dato personale e dato sulla salute o l'eventuale cifratura.
Qualora esistano Database sviluppati con software non adatto (per esempio Microsoft Access, che è valido per gestire dati non sensibili o per realizzare query di interrogazione dati o maschere di interfaccia, ma non è adatto alla gestione di tabelle di dati sensibili), in attesa di una migrazione su piattaforme adeguate, l'amministratore di banca dati specifica adotta comunque le misure di sicurezza seguendo la seguente procedura:

- *supporto fisico degli archivi*

Gli archivi, che contengono dati sensibili devono essere riposti, ogni volta che si è terminato il trattamento o comunque alla fine della giornata di lavoro, in cartelle criptate sul file-server centrale (FileServer) e devono essere eliminate tutte le altre eventuali copie.
Per creare una cartella criptata occorre spostarsi sulla propria cartella di FileServer, creare all'interno una nuova cartella, cliccarci con il tasto destro, scegliere proprietà e nel Tab. *"generale"* cliccare sul pulsante *"avanzate"* e spuntare la voce *"crittografa contenuto per la protezione dei dati"*;

- *accesso degli incaricati*

Per garantire l'accesso agli incaricati dei profili E e G, l'amministratore di banca dati specifica può permettere agli incaricati di lavorare sul Database, consentendo l'accesso ai file crittografati solo per il tempo necessario all'espletamento delle funzioni.
Per consentire l'accesso ad un file crittografato è necessario cliccarci con il tasto destro, scegliere proprietà e nel Tab. *"generale"* cliccare sul pulsante *"avanzate",* cliccare sul pulsante *"Dettagli"* ed aggiungere l'utente all'elenco di coloro che possono accedere al file.
La stessa procedura deve essere usata per revocare il permesso.

3.3.1.4 <u>*Utente banca dati centrale D*</u>

Questo profilo viene assegnato agli utenti della banca dati denominata "Centrale".
Gli incaricati con questo profilo hanno accesso alle banche dati senza poterne apportare modifiche.

- <u>*modalità di accesso (autenticazione, cambio password, ecc...)*</u>

L'accesso alla banca dati centrale viene gestito dagli incaricati con profilo A.
Ogni utente accede alla banca dati attraverso un sistema di autenticazione che prevede un nome utente e una password personali e non cedibili.
E' obbligatorio sostituire la propria password di accesso ogni 3 mesi (al massimo).
Con questo tipo di autenticazione si accede ai dati sensibili e ai dati sensibili criptati.

- *Come accedere ai dati sensibili (comunicazione inizio e fine trattamento)*

Qualora sia necessario conoscere i dati personali in chiaro è obbligatorio farne richiesta (via e-mail) agli incaricati di Profilo A, che renderanno visibili per il tempo necessario al trattamento le banche dati richieste.
Si raccomanda, pertanto, di comunicare tempestivamente la fine del trattamento.

Gestione delle porzioni di archivi sensibili fino alla fine del trattamento
Qualora ai fini del trattamento sia necessario estrarre e trasferire, sul proprio pc, porzioni del database centrale contenenti dati sensibili, al termine del trattamento o della giornata di lavoro devono essere rimossi dal proprio PC e spostati in una cartella criptata collocata nella propria directory di DocServer.
Per creare una cartella criptata occorre spostarsi sulla propria cartella di DocServer, creare una nuova cartella, cliccarci con il tasto destro, scegliere proprietà e nel Tab. *"generale"* cliccare sul pulsante *"avanzate"* e spuntare la voce *"crittografa contenuto per la protezione dei dati".*
Tale operazione, ovviamente, non è necessaria per porzioni di archivio che non includono dati sensibili.

3.3.1.5 Utente banca dati specifica E

Questo profilo viene assegnato agli utenti delle banche dati specifiche.
Gli incaricati con questo profilo hanno accesso alle banche dati senza poterne apportare modifiche.

- *Modalità di accesso*

L'accesso alla banca dati specifica viene gestito dagli incaricati con profilo C.

- *Gestione delle porzioni di archivi sensibili fino alla fine del trattamento*

Qualora ai fini del trattamento sia necessario estrarre e trasferire, sul proprio pc, porzioni dell'archivio contenente dati sensibili, al termine del trattamento o della giornata di lavoro devono essere rimossi dal proprio pc e spostati in una cartella criptata collocata nella propria directory di DocServer.
Per creare una cartella criptata occorre spostarsi sulla propria cartella di DocServer, creare una nuova cartella, cliccare sulla stessa con il tasto destro, scegliere proprietà e nel Tab. *"generale"* cliccare sul pulsante *"avanzate"* e spuntare la voce *"crittografa contenuto per la protezione dei dati".*

3.3.1.6 Operatore inserimento Dati G

Questo profilo viene assegnato agli operatori delle banche dati specifiche che devono svolgere attività di inserimento dati.
Gli incaricati con questo profilo hanno accesso alle banche dati solo per fare modifiche e/o nuovi inserimenti dati.

- *Modalità di accesso*

L'accesso alla banca dati specifica viene gestito dagli incaricati con profilo C.
Il profilo in oggetto non è autorizzato a eseguire elaborazioni o estrazioni dall'archivio ma solo ad apportare modifiche o eseguire nuovi inserimenti.

3.3.1.7 Operatore segreteria H

Questo profilo viene assegnato al personale addetto alla segreteria, al protocollo, alla logistica, reception e servizio pulizie. Qualora, nell'ambito dello svolgimento dei propri compiti, il personale in oggetto prenda visione di dati sensibili si raccomanda il pieno rispetto delle prescrizioni generali e dei principi del codice in materia di dati sensibili. In particolare:

- *Gestione del protocollo*

Nell'ambito dell'attività è necessario archiviare solo le porzioni di informazione non sensibile provvedendo all'occultamento o all'omissione di eventuali allegati contenente informazioni sensibili.

- *Invio richiesta dati sensibili*

Qualora nell'ambito dell'attività si debba richiedere a soggetti/enti esterni ad ARS documenti contenenti dati sensibili è necessario allegare alla richiesta la formulazione di cui *all'Allegato 4/A*.

Inoltre occorre indicare a soggetti/enti suddetti le modalità per la trasmissione dei dati in oggetto al fine di garantire la tutela della riservatezza dei dati inviati.
Le modalità di trasmissione ammesse sono:

- ✓ posta ordinaria in busta chiusa con dizione *"Riservato"* e nominativo del destinatario;
- ✓ consegne manuali;
- ✓ trasmissione criptata di dati;
- ✓ ax con indicazione del destinatario.

Si ricorda che tale attività è limitata ai dati in entrata, mentre è fatto assoluto divieto di trasmissione all'esterno di dati sensibili se non preventivamente autorizzata dal Responsabile del trattamento.

Istruzioni specifiche per gli incaricati della struttura tecnico amministrativa della Direzione

I paragrafi seguenti sono finalizzati a fornire le prescrizioni agli incaricati che operano all'interno della struttura tecnico-amministrativa assegnata funzionalmente alla Direzione, con lo sforzo di contestualizzare il più possibile le relative indicazioni. L'intento è quello di fornire un prodotto operativo e ampiamente fruibile per le singole strutture, attraverso il processo di applicazione della norma generale ed astratta alle dinamiche concrete di ogni singola struttura.
La prima parte presenta una breve introduzione degli adempimenti che gravano sui settori esaminati, esplicitando le motivazioni, l'importanza che riveste la corretta applicazione del Codice e aggiornamenti sull'argomento.
La seconda parte, invece, offre uno strumento operativo, che indica, per le più rilevanti azioni quotidiane le operazioni che gli incaricati dovranno compiere in attuazione delle disposizioni del Codice, strettamente correlate al profilo di autorizzazione loro assegnato.

3.4.1 Principi e disposizioni generali

I profili relativi alla tutela della riservatezza nelle pubbliche amministrazioni afferiscono in particolar modo agli uffici cui compete la gestione del personale. Questi ultimi detengono ed acquisiscono un numero elevato di informazioni relative ai dipendenti dell'amministrazione, derivando da ciò la necessità di una preliminare ricognizione delle proprie attività alla luce delle norme vigenti che deve essere costantemente aggiornata.
In generale, nel titolo VIII Parte II del Codice, *"Lavoro e previdenza sociale",* l'art. 112, considera di rilevante interesse pubblico una serie di trattamenti di dati sensibili e giudiziari attinenti ai lavoratori e finalizzati all'instaurazione e alla gestione da parte di soggetti pubblici di rapporti di lavoro di qualunque tipo dipendente o autonomo, anche non retribuito o onorario o a tempo parziale o temporaneo e di altre forme di impiego che non comportano la costituzione di un rapporto di lavoro subordinato. In particolare tali trattamenti sono quelli effettuati al fine di:

- ✓ verificare il possesso di particolari requisiti previsti per l'accesso a specifici impieghi, o la sussistenza dei presupposti per la sospensione o la cessazione dall'impiego o dal servizio (art. 112, comma 2, lett. c));
- ✓ adempiere agli obblighi connessi alla definizione dello stato giuridico ed economico del personale, nonché ai relativi obblighi retributivi, fiscali e contabili (lett. d));
- ✓ adempiere a specifici obblighi o compiti previsti in materia di igiene e sicurezza del lavoro (lett. e));
- ✓ svolgere attività dirette all'accertamento della responsabilità civile, disciplinare e contabile dei dipendenti (lett. g)).

In primo luogo occorre ribadire, come in precedenza precisato, come gli uffici dovranno sempre operare utilizzando i due principi cardini della **necessità e della pertinenza e non eccedenza**. Essi informeranno la loro azione alle regole generali indicate per il trattamento dei dati negli articoli da 11 a 17 del Codice. Sono individuati i profili di

legittimità del trattamento dei dati e, in funzione di completa garanzia, il trattamento dei dati operato in modo difforme dalle prescrizioni indicate è sanzionato con l'impossibilità dell'utilizzo dei medesimi.
Rispetto a tale profilo è opportuno ricordare che il Codice assicura l'operatività delle sue disposizioni rendendo più stringente ed incisiva la responsabilità civile, che grava in capo ai pubblici dipendenti, con la espressa previsione dell'obbligo del risarcimento del danno ex articolo 2050 del codice civile a carico di coloro che cagionano un danno ad altri a causa del trattamento dei dati personali e con la previsione della risarcibilità per danno non patrimoniale anche in caso di violazione delle disposizioni relative alle modalità del trattamento di cui all'articolo 11.
Appare utile ricordare anche in questa sede, come più volte precisato, che il trattamento dei dati sensibili da parte di soggetti pubblici, quindi da parte di ARS, è consentito solo se autorizzato da espressa disposizione di legge nella quale sono specificati i tipi di dati che possono essere trattati e di operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite[43].
Come specificato in seguito, pertanto, ARS, in quanto ente pubblico, può trattare i dati relativi al rapporto di lavoro dei propri dipendenti in quanto attività di rilevante interesse pubblico, prevista da legge; in particolare: d.lgs. 165/2001; Stat. Lav.; legge n. 53/2000; contratti collettivi nazionali di lavoro comparto regioni e autonomie locali e dirigenza; d.p.r. 1032/1973; legge 335/1995; d.lgs. 151/2001; legge 335/1995; d.p.r. 1092/1973; d.lgs. 503/1992; d.lgs. 151/2001; legge 1204/1971.
ARS per le stesse ragioni può trattare i dati che derivano dall'attività di gestione del patrimonio e contabilità, in virtù delle seguenti disposizioni: legge 241/1990 come modificata dalla legge 15/2005; legge 20 marzo 1865 n. 2248 All. F; legge 205/2000, legge 286/1999; d.lgs. 157/1995; Direttiva 2004/18/CE, nuovo Codice dei contratti pubblici (d.lgs. 163/2006 e ss.mm.).

Si riassumo, di seguito, le principali disposizioni impartire per le Pubbliche Amministrazioni, raccomandando che per le prescrizione ivi contenute si deve fare esplicito riferimento a quanto precisato nei paragrafi che precedono.

3.4.1.1 Direttiva Dipartimento Funzione Pubblica 11 febbraio 2005, n. 1 (pubblicata in G.U. 28/04/2005, n. 97)

Il Dipartimento della Funzione Pubblica con la direttiva n. 1/2005 ha provveduto ad indicare le misure finalizzate all'attuazione nelle pubbliche amministrazioni delle disposizioni contenute nel d.lgs. n. 196/2003, con particolare riguardo alla gestione delle risorse umane. Come già ricordato, il trattamento dei dati personali da parte delle pubbliche amministrazioni è consentito solo per lo svolgimento delle funzioni istituzionali; i dati sensibili possono essere trattati soltanto se il trattamento risulta autorizzato da un'espressa disposizione di legge, nella quale sono specificati i tipi di

43 L'art. 20 precisa che "*Nei casi in cui una disposizione di legge specifica la finalità di rilevante interesse pubblico, ma non i tipi di dati sensibili e di operazioni eseguibili, il trattamento è consentito solo in riferimento ai tipi di dati e di operazioni identificati e resi pubblici a cura dei soggetti che ne effettuano il trattamento, in relazione alle specifiche finalità perseguite nei singoli casi e nel rispetto dei principi di cui all'articolo 22, con atto di natura regolamentare adottato in conformità al parere espresso dal Garante ai sensi dell'articolo 154, comma 1, lettera g), anche su schemi tipo.*
Se il trattamento non è previsto espressamente da una disposizione di legge i soggetti pubblici possono richiedere al Garante l'individuazione delle attività, tra quelle demandate ai medesimi soggetti dalla legge, che perseguono finalità di rilevante interesse pubblico e per le quali è conseguentemente autorizzato, ai sensi dell'articolo 26, comma 2, il trattamento dei dati sensibili. Il trattamento è consentito solo se il soggetto pubblico provvede altresì a identificare e rendere pubblici i tipi di dati e di operazioni nei modi di cui al comma 2.
L'identificazione dei tipi di dati e di operazioni di cui ai commi 2 e 3 è aggiornata e integrata periodicamente".

dati che possono essere trattati, le operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite.
Per l'attuazione pratica delle previsioni del Codice in materia di protezione dei dati personali le amministrazioni devono, pertanto, adottare alcuni strumenti, in particolare:

→ regolamenti indicanti i tipi di dati sensibili e giudiziari che possono essere trattati e le operazioni, che possono essere eseguite su di essi in relazione al perseguimento di finalità di rilevante interesse pubblico qualora manchi una specifica indicazione legislativa (**articoli 20, 21 e 22**);
→ informative all'interessato (**art. 13**);
→ notificazione al Garante nei casi previsti dall'art. 37;
→ eventuali comunicazioni al Garante (**art. 39**);
→ misure minime di sicurezza e, in particolare, il documento programmatico sulla sicurezza (**art. 34, comma 1, lettera g) e regola n. 19 dell'allegato B al Codice**).

In particolare, quando una disposizione di legge abbia specificato le finalità di rilevante interesse pubblico, ma non i tipi di dati sensibili e giudiziari che possono essere trattati e le operazioni che possono essere svolte su di essi, le amministrazioni dovranno adottare un apposito regolamento con il quale identificare e rendere pubblici, a cura dei soggetti che ne effettuano il trattamento, i tipi di dati utilizzabili e le operazioni eseguibili, in relazione ai fini istituzionali perseguiti e nel rispetto dei principi affermati dall'art. 22 del Codice.[44]

ADEMPIEMENTI ANNUALI

1° gennaio di ogni anno

(1) Aggiornare l'individuazione dell'ambito di trattamento consentito ai singoli incaricati, ove variato, anche parzialmente.
(2) Verificare la sussistenza delle condizioni per la conservazione delle autorizzazioni per l'accesso ai dati particolari per gli incaricati.
(3) Fornire istruzioni organizzative e tecniche affinché il salvataggio dei dati sia effettuato settimanalmente.
(4) Programmare interventi di formazione per gli incaricati del trattamento.
(5) Provvedere all'aggiornamento delle "patch" dei programmi per computer, nel caso di trattamento di dati comuni (punto 17, Allegato B).

31 marzo di ogni anno

(1) Aggiornare il Documento Programmatico sulla Sicurezza[45].
(2) All'interno del Documento Programmatico sulla Sicurezza, deve essere previsto un piano di formazione per gli incaricati, che dovrà pertanto essere rivisto annualmente. Il piano impone che siano fatte previsioni effettive sui tempi di formazione e sulle strutture che gestiranno tali attività, nell'arco dell'anno. La formazione è programmata al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o introduzione di nuovi significativi strumenti, rilevanti per il trattamento dei dati personali.

ADEMPIMENTI SEMESTRALI

1° gennaio e 1° luglio di ogni anno

(1) Aggiornare i software antivirus, per tutti i tipi di dati.
(2) Provvedere all'aggiornamento delle "patch" dei programmi per computer, nel caso di trattamento di dati sensibili.

[44] In materia si fa esplicito riferimento a quanto precisato al precedente Capo II, paragrafi: 2.1.2.3 e 2.3.1.
[45] Come riportato al paragrafo 2.3.2, ARS ha provveduto ad aggiornare il Documento programmatico della sicurezza entro il 31 marzo di ogni anno, dandone notizia nella relazione di accompagnamento al bilancio d'esercizio dell'ARS.

3.4.1.2 Deliberazione Garante n. 23 del 14 giugno 2007 "Linee guida in materia di trattamento di dati personali dei lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico"

Le principali tematiche affrontate dalla direttiva in parola sono le seguenti:

- *Assenze per malattia, certificati e visite mediche*
  In caso di assenza per malattia all'amministrazione vanno consegnati certificati medici privi di diagnosi e con la sola indicazione dell'inizio e della durata dell'infermità. Se il lavoratore produce documentazione in cui è presente anche la diagnosi, l'ufficio deve astenersi dall'utilizzare queste informazioni e deve invitare il personale a non produrre altri certificati con le stesse caratteristiche. Particolari cautele devono essere adottate dall'ente pubblico quando tratta dati sulla salute dei dipendenti nei casi di visite medico legali, denunce di infortunio all'Inail, abilitazioni al porto d'armi e alla guida.
- *Diffusione dei dati in Internet*
  Le amministrazioni devono assicurare l'esattezza, l'aggiornamento e la pertinenza dei dati pubblicati in rete e garantire il "*diritto all'oblio*", cioè una tutela dinamica della riservatezza delle persone (trascorso un certo periodo dalla pubblicazione è opportuno spostare i nominativi in una parte del sito dove non siano più rintracciabili dai motori di ricerca esterni). Nelle graduatorie relative a concorsi o selezioni vanno riportati solo dati pertinenti (elenchi nominativi abbinati ai risultati, elenchi di ammessi alle prove scritte o orali, no a recapiti telefonici, codice fiscale ecc.) É sempre vietata la diffusione di informazioni sulla salute del lavoratore o dei familiari interessati.
- *Dati biometrici dei lavoratori pubblici*
  Anche nell'ambito del pubblico impiego non è consentito un uso generalizzato dei dati biometrici dei dipendenti (impronte digitali, iride) per controllare le presenze o gli accessi sul luogo di lavoro. Il Garante può autorizzare l'attivazione di tali sistemi di rilevazione solo in presenza di particolari esigenze (aree adibite alla sicurezza dello Stato, torri di controllo, conservazione di oggetti di particolare valore) e con precise garanzie (verifica preliminare dell'Autorità, no ad archivi centralizzati, codice cifrato dell'impronta memorizzato solo nel badge del dipendente).
- Comunicazioni tra amministrazione e lavoratore
  Per prevenire la conoscenza ingiustificata di dati da parte di persone non autorizzate, l'amministrazione deve adottare forme di comunicazione con il dipendente protette e individualizzate: inoltrando le note in busta chiusa, inviandole all'e-mail personale o invitandolo a ritirare personalmente la documentazione.

3.4.2 Il rapporto di lavoro e la Privacy

3.4.2.1 Principi generali

Si ritiene opportuno esporre una breve sintesi relativa all'influenza del Codice privacy in materia di rapporto di lavoro, ribadendo alcune prescrizioni già impartite nei paragrafi che precedono; il Codice, infatti, individua alcuni principi fondamentali:

a) i dati devono essere innanzitutto raccolti "*per scopi specifici, espliciti e legittimi*";
b) al lavoratore deve essere garantita la massima trasparenza sulla raccolta e sull'uso dei propri dati da parte del datore di lavoro, nonché il diritto di rettifica ed integrazione delle informazioni;
c) i dati raccolti ed usati dal datore di lavoro devono essere "esatti, aggiornati e strettamente indispensabili";
d) il datore di lavoro deve garantire la sicurezza dei dati dei lavoratori adottando misure tecnologiche ed organizzative a protezione dei dati, specie avuto riguardo ad accessi illeciti;
e) il trasferimento di dati dei lavoratori all'esterno della UE è possibile solo se il Paese di destinazione assicura un adeguato livello di protezione verificato dal datore di lavoro;
f) ogni controllo dei dati personali dovrà essere oggetto di una preventiva informativa agli interessati; dovrà inoltre essere proporzionato e rispettoso della privacy e di altri interessi dei lavoratori.

Sanzioni previste[46]

a. Multe da 3.000 a 50.0000 euro (elevabile al triplo);
b. reclusione fino a 3 anni;
c. possibilità di estinguere il reato penale, adeguandosi alla normativa e pagando una sanzione pecuniaria.

3.4.2.3 Casi specifici

Diritti del lavoratore.
Il lavoratore può chiedere al datore di sapere come e perché utilizzi i propri dati personali, quelli riferibili a soggetti identificati o identificabili ed eventualmente intervenire per correggerli, integrarli o aggiornarli se inesatti, incompleti o vecchi oppure cancellarli se trattati in violazione della legge. E' vietato il controllo a distanza del lavoratore attraverso impianti audiovisivi.
Gli adempimenti per il datore di lavoro.
Sono essenzialmente **tre gli adempimenti** cui é tenuto il datore di lavoro nei confronti del lavoratore. Innanzitutto l'informativa, un atto di trasparenza in cui si dichiara come e perché vengono trattati i dati degli interessati e se saranno trasmessi a terzi, oltre a ricordare i diritti esercitabili. Il datore dovrà poi ottenere il consenso del lavoratore al trattamento dei dati, che può essere espresso verbalmente purché

[46] Si faccia anche riferimento a quanto precisato nel Capo I, paragrafo 1.4.

documentato per iscritto ma non é necessario in caso di obblighi fiscali o contributivi stabiliti dalla legge.

Dati sensibili.

Nelle comunicazioni concernenti l'adozione di provvedimenti di gestione interna del personale (trasferimenti o avvicendamenti), sono riportati dati di carattere sensibile riguardanti, in particolare, la salute di dipendenti. Il trattamento di queste informazioni, per perseguire una rilevante finalità d'interesse pubblico di gestione di rapporti di lavoro, può in generale ritenersi lecito. Occorre, tuttavia, che siano rispettati anche i principi di proporzionalità, necessità, pertinenza e non eccedenza dei dati, limitando il trattamento, in ogni sua fase, alle sole informazioni strettamente indispensabili al raggiungimento di tale finalità (artt. 11 e 22 del Codice)[47].

Organizzazione degli uffici.

L'entrata in vigore del nuovo Codice comporta per le Pubbliche Amministrazioni la necessità di ripensare le proprie attività e la propria organizzazione, così da consentire una piena ed effettiva garanzia dei diritti in esso affermati.

Le tematiche relative alla privacy, infatti, investono le Amministrazioni nella quasi totalità delle proprie attività, assumendo significativo rilievo nello svolgimento di molti compiti istituzionali loro affidati dall'ordinamento.

Alcuni specifici obblighi normativi impongono alle amministrazioni pubbliche di rendere noti, attraverso i propri siti Internet, determinati dati personali concernenti i propri dipendenti (es. organigramma degli uffici con l'elenco dei nominativi dei dirigenti; elenco delle caselle di posta elettronica istituzionali attive).

Tali dati, sebbene siano di fatto disponibili in Internet, possono essere utilizzati da terzi (in particolare, gli indirizzi di posta elettronica) **solo in relazione ad eventi, comunicazioni e scopi correlati alle funzioni istituzionali e al ruolo ricoperto dall'interessato all'interno dell'amministrazione.**

Tali stessi dati **non sono** quindi **utilizzabili liberamente da chiunque** per inviare, ad esempio, comunicazioni elettroniche a contenuto commerciale o pubblicitario.

Se pensiamo alla disciplina sul riordino della dirigenza statale, poi, le amministrazioni dello Stato possono altresì diffondere in Internet i dati personali dei dirigenti inquadrati nei ruoli istituiti da ciascuna amministrazione (art. 23 d.lgs. 30 marzo

[47] A titolo esemplificativo, non è stata così ritenuta rispondente al principio di necessità l'indicazione, nelle comunicazioni indirizzate alle sedi interessate, dei gravi motivi di salute su cui era fondato il provvedimento di trasferimento di un dipendente. Il trasferimento, infatti, avrebbe potuto essere comunicato a tali uffici mediante una nota contenente, in sintesi, il testo del provvedimento originario e gli estremi di riferimento del provvedimento. Tale accorgimento, peraltro, non pregiudica l'obbligo di adeguata motivazione degli atti amministrativi (art. 3, comma 3, l. n. 241/1990), né la facoltà delle persone a ciò legittimate di accedere ad eventuali altri dati, anche di tipo sensibile, contenuti in tali atti, in conformità alle leggi e ai regolamenti in materia di accesso alla documentazione amministrativa.
In materia di trattamento di dati sensibili, il Garante ha ritenuto che la disciplina sulla protezione dei dati personali non ponesse ostacoli di fondo ad un'iniziativa del Ministero degli affari esteri consistente nell'identificare i dipendenti portatori di handicap ai fini di esercitazione per evacuazioni antincendio in conformità alla disciplina sull'igiene e la sicurezza del lavoro.
Tale attività rientra infatti tra quelle che, sulla base del Codice, possono giustificare il trattamento di dati sensibili (artt. 86, comma 1, lett. c) e 112, comma 2, lett. e) del Codice). Nel ricordare, anche in questo caso, che l'amministrazione può effettuare il trattamento delle informazioni relative allo stato di disabilità dei dipendenti soltanto se esse sono realmente "indispensabili per svolgere attività istituzionali che non possono essere adempiute, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa" (art. 22, comma 3, del Codice), dovendo altresì rispettare le regole di proporzionalità, indispensabilità, pertinenza e non eccedenza, si è fatto presente al Ministero che, per questa ed altre attività di trattamento di dati sensibili, è necessario provvedere con atto regolamentare ad individuare i tipi di dati che possono essere trattati e le operazioni eseguibili (art. 20, comma 2, del Codice).
Con specifico riferimento al trattamento dei dati sensibili nell'ambito della gestione del personale delle forze armate e di polizia, su richiesta della Guardia di finanza, l'Autorità si è espressa in merito all'utilizzo di test psicoattitudinali nelle procedure concorsuali di reclutamento (Nota 3 giugno 2004).

2001, n. 165), nel rispetto dei principi di completezza, esattezza, aggiornamento, pertinenza e non eccedenza dei dati (art. 11 del Codice Privacy).
Altre disposizioni di settore prevedono, inoltre, specifici regimi di pubblicità per talune informazioni personali concernenti le retribuzioni, i livelli stipendiali o le situazioni patrimoniali di titolari di cariche e incarichi pubblici.

Concorsi.

Il Garante, con Nota 25 agosto 2004 ha dichiarato che non costituisce violazione della disciplina sulla riservatezza la richiesta, rivolta dalle amministrazioni pubbliche agli aspiranti, di una dichiarazione sostitutiva dei carichi pendenti.
Tale procedura tiene conto dell'esigenza dell'amministrazione di verificare l'eventuale presenza di cause ostative all'accesso al pubblico impiego (art. 85, decreto del Presidente della Repubblica del 10 gennaio 1957, n. 3 e art. 2, decreto del Presidente della Repubblica del 9 maggio 1994, n. 487); esigenza quest'ultima espressamente riconosciuta dall'art. 71 del decreto del Presidente della Repubblica n. 445/2000 e dalla recente riforma del casellario giudiziale, che prevede anche una forma di accesso diretto alla banca dati da parte delle amministrazioni (decreto del Presidente della Repubblica del 14 novembre 2002, n. 313).
Con la deliberazione n. 23 del 14 giugno 2007, il Garante ha provveduto ad enucleare le "*Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico".*
In particolare in materia di dati relativi a concorsi e selezioni ha predisposto alcune indicazioni che assumono la portata di un onere a carico della pubblica amministrazione e specificatamente:

- le graduatorie dei vincitori di concorsi per accedere agli impieghi nelle pubbliche amministrazioni o per attribuire specifici incarichi professionali devono essere pubblicate nel bollettino ufficiale della Presidenza del Consiglio dei ministri o dell'amministrazione interessata, dandone, se previsto, contestuale avviso sulla Gazzetta Ufficiale;
- la diffusione, che l'amministrazione può lecitamente porre in essere in base a specifiche previsioni legislative o regolamentari, deve avere ad oggetto solo i dati personali pertinenti e non eccedenti ai fini del corretto espletamento della procedura concorsuale e della sua rispondenza ai parametri stabiliti nel bando (elenchi nominativi ai quali vengano abbinati i risultati di prove intermedie, elenchi degli ammessi alle prove scritte o orali, punteggi riferiti a singoli argomenti di esame; punteggi totali ottenuti). Altre tipologie di informazioni non pertinenti quali, ad esempio, recapiti di telefonia fissa o mobile o il codice fiscale, **sono illecite**;
- lecita è la ricezione on-line di domande di partecipazione a concorsi e selezioni, corredate di diversi dati personali. A tale proposito va rilevato che le previsioni normative che disciplinano la pubblicazione di graduatorie, esiti e giudizi concorsuali rendono, in linea generale, lecita l'operazione di diffusione dei relativi dati personali a prescindere dal mezzo utilizzato. A tal proposito, vista la possibilità consentita a chiunque di accedere alle informazioni personali rese disponibili in rete, per effetto dei comuni motori di ricerca esterni ai siti, **occorre prevedere forme adeguate di selezione delle informazioni che potrebbero essere altrimenti aggregate massivamente mediante un comune motore di ricerca esterno ai siti.** Il Garante suggerisce quali soluzioni possibili:
  - ✓ l'accesso alle pagine web contenenti dati relativi a esiti, graduatorie e giudizi di valutazione solo consultando un determinato sito Internet;

- ✓ l'attribuzione solo alle persone interessate di una chiave personale di accesso (a vari dati relativi alla procedura, oppure solo a quelli che li riguardano);
- ✓ la predisposizione, nei siti istituzionali, di aree ad accesso parimenti selezionato nelle quali possono essere riportate ulteriori informazioni accessibili anche ai controinteressati;

Stato di salute lavoratore.

Nel fascicolo del dipendente pubblico è ammessa la conservazione dei dati inerenti alla sua salute in quanto richiesta espressamente da alcune disposizioni di legge. Dunque, ai sensi dell'art. 26, comma 4 lett. d) del Codice, il trattamento di tali dati può essere effettuato senza il consenso dell'interessato.

Dovranno, tuttavia, essere rispettate le regole che saranno previste dall'adottando codice di deontologia e buona condotta, nonché della autorizzazione generale annualmente rilasciata dal Garante.

Il Garante ha altresì verificato la liceità delle segnalazioni trasmesse da medici all'Inail circa le malattie riscontrate nei pazienti, collegabili allo svolgimento di attività lavorative. Sul punto si è precisato che, secondo il quadro normativo vigente (decreto del Presidente della Repubblica n. 1124/1965; decreto ministeriale del 18 aprile 1973 e decreto legislativo n. 38/2000), il medico può trasmettere all'istituto assicuratore e ad altri organismi preposti le segnalazioni di malattie professionali che potrebbero essere state causate da un'attività lavorativa potenzialmente nociva, indicandone l'anamnesi lavorativa, i rischi e le sostanze cui il lavoratore sia (o sia stato) esposto. Questa comunicazione deve essere però effettuata nel rispetto delle specifiche disposizioni in tema di assicurazioni contro gli infortuni sul lavoro e le malattie professionali, nonché del principio di pertinenza dei dati rispetto alle finalità per cui sono raccolti e successivamente trattati.

Le linee guida di cui alla deliberazione Garante n. 23/2007 prevedono, tra l'altro, alcune indicazioni circa i trattamenti di dati connessi alla disciplina in materia di igiene e sicurezza del lavoro (art. 1, commi 1 e 2, d.lgs. n. 626/1994 e successive modificazioni e integrazioni).

In questo ambito il medico competente effettua accertamenti preventivi e periodici sui lavoratori (art. 33 d.P.R. n. 303/1956; art. 16 d.lgs. n. 626/1994) e istituisce (curandone l'aggiornamento) una cartella sanitaria e di rischio (in conformità alle prescrizioni contenute negli artt. 17, 59-*quinquiesdecies*, comma 2, lett. b), 59-*sexiesdecies*, 70, 72-*undecies* e 87 d.lgs. n. 626/1994).

Detta cartella è custodita presso l'amministrazione "con salvaguardia del segreto professionale" e consegnata in copia al lavoratore stesso al momento della risoluzione del rapporto di lavoro, ovvero quando lo stesso ne fa richiesta" (artt. 4, comma 8, e 17, comma 1, lett. d), d.lgs. n. 626/1994); in caso di cessazione del rapporto di lavoro le cartelle **sono trasmesse all'Istituto superiore prevenzione e sicurezza sul lavoro-Ispesl** (artt. 59-*sexiesdecies*, comma 4, 70, comma 4, 72-*undecies,* comma 3 e 87, comma 3, lett c), d.lgs. n. 626/1994), in originale e in busta chiusa.

Alle predette cartelle **il datore di lavoro non può accedere**, **dovendo soltanto concorrere ad assicurarne un'efficace custodia nei locali dell'amministrazione** (anche in vista di possibili accertamenti ispettivi da parte dei soggetti istituzionalmente competenti) ma, come detto, "con salvaguardia del segreto professionale".

Il datore di lavoro pubblico **è tenuto, su parere del medico competente (o qualora quest'ultimo lo informi di anomalie imputabili all'esposizione a rischio), ad adottare le misure preventive e protettive per i lavoratori interessati**; in questo specifico contesto

il datore di lavoro può accedere al giudizio di idoneità del lavoratore allo svolgimento di date mansioni, anziché alle specifiche patologie accertate.

Fascicolo del dipendente.

Il Garante per la protezione dei dati personali (Newsletter n. 11 del 17 ottobre 2004) ha reso noto di essere intervenuto in una questione inerente l'indebita diffusione di lettere contenente dati personali di una lavoratrice e di sua figlia disabile e di aver stabilito che il datore di lavoro, sia esso pubblico che privato, deve trattare e conservare i dati dei propri dipendenti nel pieno rispetto del diritto alla protezione dei dati, adottando anche, a pena di sanzioni civili e penali, ogni idonea misura di sicurezza per prevenire eventi lesivi della privacy. Il Garante ha inoltre precisato che la tutela deve essere maggiormente garantita nel caso in cui tra le informazioni raccolte compaiono dati sensibili riferiti a un minore. Con questa decisione l'Autorità Garante ha accolto il ricorso di una dipendente di una società che lamentava una grave violazione della propria riservatezza personale e familiare ordinando alla società, oltre che di astenersi dall'ulteriore trattamento illecito dei dati personali dell'interessata, anche di adottare tutte le misure di sicurezza idonee a prevenire il ripetersi di eventi del genere.

Anche in questo ambito, pertanto, si deve operare secondo il principio di necessità e di pertinenza e non eccedenza, inoltre debbono essere poste in essere tutte le misure idonee a garantire la sicurezza nella tenuta dei fascicoli, soprattutto se gestiti informaticamente.

Buoni pasto.

Sul tema si propone la questione dell'indicazione di dati personali dei lavoratori nei buoni pasto (in particolare, i nominativi dei singoli beneficiari e la loro sede di servizio), accanto alle informazioni sul datore di lavoro, nonché dei presupposti di liceità per comunicare i dati dei dipendenti al soggetto tenuto all'erogazione del servizio.

Sebbene il garante non si sia ancora espresso a tal proposito, seppur sollecitato da parte di diverse PP.AA., è possibile dedurre che, per il trattamento di tali dati, sia necessario verificare, alla luce del contratto tra le parti, il rispetto del principio di non eccedenza del trattamento rispetto alle finalità della raccolta, affermato nell'art. 11 del Codice privacy.

Nel caso in cui dovesse essere verificata la fattibilità della cosa, occorrerebbe, comunque, informare l'interessato ed acquisirne il consenso espresso.

Inoltre, si segnala la necessità di ricordare che il cedolino contiene dati che debbono rimanere riservati. Pertanto anche gli uffici competenti, in sede di compilazione del cedolino, dovranno tener presenti le disposizioni del Codice ed eventualmente sostituire le voci specifiche con voci generiche.

Le visite fiscali.

Le visite fiscali non violano la privacy, in quanto disposizioni di legge e contrattuali prevedono la possibilità di tali controlli anche in caso di brevi assenze e le PP.AA., ove il trattamento sia necessario, pertinenti ed indispensabile, potrà provvedere a comunicare i dati alle strutture e medici competenti.

Uso delle impronte digitali per controllare le presenze dei lavoratori.

Il Garante privacy con un proprio provvedimento (Nota del 21 Luglio 2005) ha vietato l'uso generalizzato delle impronte digitali dei dipendenti per controllare le presenze sul luogo di lavoro, ritenendo tale sistema troppo invasivo della sfera personale e della libertà individuale. Del resto, per raggiungere lo stesso scopo si possono adottare altre tecniche più proporzionate ed ugualmente efficaci.

Test psico-attitudinali.

Il divieto di trattare informazioni sensibili nell'ambito di test psico-attitudinali previsto dal Codice (art. 22, comma 10) si riferisce anche alla raccolta di questi dati mediante questionari volti a costruire il profilo o la personalità dell'interessato. Va pertanto espunta dai questionari utilizzati sia per gli esami psico-attitudinali, sia per quelli psichiatrici, ogni domanda idonea a rivelare profili particolarmente delicati della sfera privata dell'interessato, quali la salute, le abitudini sessuali, le convinzioni politiche, sindacali, religiose, filosofiche o d'altro genere. A seconda degli esiti di tali esami è invece possibile procedere ad ulteriori accertamenti, ove ritenuto indispensabile, purché questi non consistano nella somministrazione ai candidati di test psico-attitudinali volti a definire il loro profilo o la loro personalità mediante il trattamento di dati sensibili. In questo caso occorre rendere all'interessato una previa e specifica informativa, in modo da consentirgli di non sottoporsi alla prosecuzione della procedura concorsuale e, quindi, a tali ulteriori accertamenti (artt. 13 e 7 del Codice). Nel trattamento di queste informazioni l'amministrazione deve rispettare comunque il principio di indispensabilità, valutando specificamente il rapporto tra i dati sensibili e gli adempimenti legati a compiti e obblighi espletati (artt. 20 e 22 del Codice). Il mancato rispetto di tali garanzie rende il trattamento illecito, anche se effettuato nello svolgimento di funzioni istituzionali o ritenute giustificate da norme di servizio e regolamenti interni.

Particolari comunicazioni:procedimento disciplinare.

La normativa in materia stabilisce che le comunicazioni relative ai procedimenti disciplinari dei pubblici dipendenti debba avvenire mediante la consegna personale all'interessato o, qualora questa non sia possibile, l'invio di una raccomandata (artt. 111 e 104, decreto del Presidente della Repubblica n. 3/1957); tuttavia, l'utilizzo del fax come mezzo di comunicazione tra amministrazioni è consentito dalla legge e, in linea generale, non è in contrasto con i principi in materia di protezione dei dati personali. Il Garante ha comunque evidenziato che per talune circostanze occorre rispettare le specifiche modalità eventualmente previste dalla normativa di settore.

Lavoro e disabili.

Il divieto di diffusione dei dati idonei a rivelare lo stato di salute è espressamente ribadito dal Codice in relazione allo svolgimento delle attività di concessione di benefici ed agevolazioni previste dalla legge e dai regolamenti.

In proposito, il Garante, con la Nota 21 settembre 2004, ha precisato che, trattandosi di informazioni idonee a rivelare lo stato di disabilità degli interessati, occorre far riferimento alla distinta e più stringente disciplina prevista per il trattamento dei dati sensibili (artt. 20 e 22 del Codice).

Una particolarità, nelle graduatorie di trasferimento la dicitura "*portatore di handicap"* come titolo di precedenza rivela a chiunque legga la graduatoria una specifica condizione di salute di alcuni lavoratori, andando a costituire, così, una forma di diffusione di dati sanitari espressamente vietata dall'ultimo comma dell'art. 26 del Codice della privacy.

La formula "*portatore di handicap*" potrà essere sostituita con diciture generiche o con codici numerici, al fine di rispettare la riservatezza dei soggetti interessati e di garantire la trasparenza dell'azione amministrativa.

Uso dei cartellini identificativi da parte dei dipendenti.

Non è contrario alla legge chiedere ai lavoratori di esporre un cartellino, al fine di renderli identificabili per finalità di trasparenza, in particolare nei rapporti con il

pubblico o con terzi estranei; tuttavia, non sempre i dati riportati su tali cartellini appaiono pertinenti e non eccedenti rispetto alle finalità del trattamento.
Non sembra, ad esempio, pertinente esibire anche la data di nascita del dipendente ovvero ogni altra informazione non strettamente necessaria, essendo sufficiente indicare il nome (anche di fantasia), un numero, un codice, che comunque permetta di risalire al dipendente in caso di necessità.
Con analoghi accorgimenti, la finalità della trasparenza sarà rispettata senza esporre il lavoratore ad un'inutile diffusione dei suoi dati personali.

Valutazione del personale.

Le raccolte di dati effettuate in occasione delle valutazioni periodiche del personale, tramite test o interviste nominative, si configurano come un trattamento di dati personali da realizzare, quindi, in conformità alle norme dettate dal Codice.
In particolare, il datore di lavoro dovrà fornire ai dipendenti da valutare una preventiva e completa informativa e potrà raccogliere le sole informazioni funzionali alla valutazione professionale del lavoratore, utilizzandole per il solo fine per il quale sono state acquisite.
Nella redazione dei moduli di valutazione deve esser tenuto conto del diritto sancito dall'articolo 1 dello Statuto dei Lavoratori, che garantisce la libertà di espressione del pensiero, tutelando anche il diritto a non manifestare una propria opinione.
Detti schemi di valutazione non dovranno, in ogni caso, costituire metodi per svolgere indagini sulle opinioni politico-sindacali del lavoratore (nel rispetto dell'art. 8 dello Statuto dei Lavoratori).
Sono dati personali le informazioni sul lavoratore annotate in schede, note di qualifica, valutazioni o altri documenti formati dal datore di lavoro, anche se tali dati, cui il lavoratore ha diritto di accedere, non sono suscettibili di correzione o rettifica in quanto espressione del libero e soggettivo convincimento del valutatore[48].

---

[48] A tal proposito si riassume una decisione del Garante resa quando ancora era vigente il d.lgs. 675/1996, ma che vale ancora quale petizione di principio. Alcuni dipendenti di Poste Italiane S.p.A. chiedono di ottenere copia di una scheda di valutazione compilata sul loro conto da parte dalla società per cui lavorano. Non ottenendo risposta i dipendenti ricorrono al Garante della privacy ai sensi dell' art. 29 della legge n. 675/1996. Il ricorso formulato induce il Garante a interpellare Poste Italiane S.p.A., che risponde che:
- è in atto un processo di riorganizzazione e ristrutturazione delle varie strutture aziendali e che è stata a tal fine attivata una procedura volta ad acquisire notizie riguardanti i dipendenti interessati, al fine "di individuare le unità con elevata potenzialità e di accertare le esigenze formative del predetto personale";
- le istanze di accesso presentate dagli interessati sono state rifiutate perché le schede in questione contengono "valutazioni soggettive del datore di lavoro e quindi riflessioni di colui che le esprime ed in quanto tali non avrebbero carattere di dato personale.";
- l'efficacia delle valutazioni comparative necessarie per garantire una gestione efficiente delle risorse umane si fondea anche sulla loro riservatezza delle schede;
- la valutazione di un datore di lavoro, consistendo in una elaborazione del tutto personale, avrebbe carattere di soggettività e, pertanto, non rientrerebbe nel novero dei dati di carattere personale, potendosi altrimenti ledere il diritto alla libertà di pensiero del datore di lavoro.
I RICORRENTI confermano le proprie richieste ribadendo il loro diritto di accedere in base alla legge n. 675/1996 ai dati personali contenuti nella scheda di valutazione richiesta, in quanto questa rappresenterebbe "il processo finale valutativo sulla base del quale l'azienda ha effettuato le scelte".
LA DECISIONE DEL GARANTE
Il Garante accoglie il ricorso dei dipendenti e ordina a Poste Italiane S.p.A. di consentire agli interessati di accedere ai dati personali agli stessi riferiti contenuti nelle schede di valutazione.
MOTIVAZIONI
L'art. 1, comma 2, lettera c), della legge n. 675/1996 definisce come dato personale "qualunque informazione relativa a persona fisica, persona giuridica " .
In base a tale specifica definizione legislativa devono essere considerate come "dato personale" tutte le informazioni di natura personale, tutti gli elementi distintivi che contribuiscono a comporre il quadro dei "dati" dell'interessato relativi alle sue attitudini, capacità, rendimento e prospettive di impiego e carriera.
Nel caso specifico tali informazioni personali provengono anche da valutazioni che restano espressione del libero e soggettivo convincimento del "valutatore" ma sono comunque soggette alla legge n. 675/1996.
L'interessato, la persona a cui si riferiscono i dati ha un diritto soggettivo a conoscere le informazioni di carattere personale che lo riguardano, anche nei casi in cui tali dati personali non siano eventualmente suscettibili di correzione in quanto contenuti nell'ambito di un giudizio o di una valutazione.
Quindi, il diritto di accesso non limita in alcun modo l'invocato "diritto alla libertà di pensiero" del datore di lavoro, poiché il diritto dell'interessato a conoscere dati che lo riguardano non comporta di per sé il diritto ad ottenere una rettifica di dati personali riportati all'interno di valutazioni rimesse al discrezionale apprezzamento del datore di lavoro.

Controllo uso telefono e/o collegamento internet non pertinente alle esigenze di servizio.

Lo Statuto dei lavoratori stabilisce i divieti dell'installazione di impianti audiovisivi o altri strumenti di controllo a distanza e di indagini sulle opinioni, a tutela del diritto alla riservatezza del dipendente sul luogo di lavoro, al fine di tutelare la libertà e la dignità dello stesso (privacy compresa).

L'impiego di strumenti di controllo a distanza (nella specie tabulati delle telefonate, i logs, ma anche i bookmarks o la cache memory) deve rispondere a precise esigenze di sicurezza e organizzazione del lavoro e deve essere comunque concordato con le rappresentanze sindacali, come previsto dallo Statuto dei Lavoratori.

Nel caso in cui tali strumenti di controllo a distanza vengano installati, sarà anche necessario rispettare i principi sanciti dal Codice sulla privacy e, in particolare, sarà, necessario fornire ai dipendenti l'informativa di cui all'art. 13, richiedere loro il consenso al trattamento dei dati e, infine, rispettare l'art. 11.

Permessi studio per esami universitari richiesta del certificato relativo all'esame sostenuto.

L'art. 10 dello Statuto dei Lavoratori prevede, all'ultimo comma, che i datori di lavoro possono richiedere la produzione delle certificazioni necessarie all'esercizio del diritto di fruire di permessi per motivi di studio.

Dal tenore letterale della disposizione, e in particolare dalla parola "necessarie", si comprende che le certificazioni devono avere il contenuto minimo idoneo a giustificare l'assenza e certamente tale non è il voto conseguito.

Nella materia è determinante l'art. 11 del Codice, che stabilisce che i dati personali oggetto di trattamento devono essere pertinenti e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati. Orbene, l'indicazione della votazione conseguita non è pertinente ed è eccedente rispetto alla finalità del trattamento che è quella di verificare il motivo dell'assenza dal posto di lavoro.

Notificazione licenziamento.

Il datore è obbligato all'adozione di misure idonee a ridurre al minimo i rischi di accesso non autorizzato alle informazioni da parte di soggetti diversi dal destinatario della comunicazione, o di trattamento non consentito o non conforme alle finalità della raccolta.

L'omessa adozione, anche solo per colpa, di idonee misure di sicurezza, se dall'episodio è scaturito un danno (anche non patrimoniale) per il soggetto interessato, consente al dipendente di ottenere il risarcimento promuovendo la relativa azione giudiziaria.

Quindi la notificazione deve avvenire tramite lettera inserita in busta chiusa, con raccomandata A.R.

Busta paga.

Il dipendente ha diritto di ottenere che la consegna della busta paga avvenga in modo tale da non permettere ai colleghi di conoscere i propri dati personali retributivi che potrebbero rivelare, oltre all'importo percepito, anche l'esistenza di particolari situazioni, quali pignoramenti in atto, assegni di mantenimento a favore del coniuge separato e così via.

Quindi la consegna deve avvenire tramite lettera inserita in busta chiusa.

3.4.2.4 Comunicazioni tra amministrazione e lavoratore.

Per prevenire la conoscenza ingiustificata di dati da parte di persone non autorizzate, l'amministrazione deve adottare forme di comunicazione con il dipendente protette e individualizzate, che possono avvenire nelle seguenti modalità:

- inoltrando le note in busta chiusa, inviandole all'e-mail personale;
- invitandolo a ritirare personalmente la documentazione.

3.4.2.5 Tabella attività

Seguono ***tabelle da 12 a 19*** riassuntive delle attività afferenti alla struttura tecnico-amministrative della Direzione, per la gestione dei rapporti di lavoro e per gli Organi, con indicazione delle fonti legislative di riferimento, della tipologia dei dati e delle operazioni eseguibili.

TABELLA ATTIVITA'

Tab. 12

RECLUTAMENTO				
Attività	**Finalità rilevante interesse pubblico**	**Fonte legislativa**	**Tipologia dati**	**Operazioni eseguibili**
Acquisizione domande	Art. 112, comma 1 e 2, lett. c), d.lgs. 196/2003	Artt. 26, 28, 29, 35, comma 1, lett. a), d.lgs. 165/2001.	Personali, sensibili, giudiziari	Raccolta Registrazione Organizzazione Conservazione Consultazione Elaborazione Selezione Estrazione Raffronto Utilizzo Blocco Cancellazione Distruzione
Espletamento prove	Art. 112, comma 1e 2, lett. c), d.lgs. 196/2003	Artt. 26, 28, 29, 35, comma 1, lett. a), d.lgs. 165/2001.	Personali e sensibili	Raccolta, Registrazione Organizzazione Conservazione Consultazione Elaborazione Selezione Estrazione Raffronto Comunicazione Utilizzo Blocco Cancellazione Distruzione
Formazione graduatoria	Art. 112, comma 1e 2, lett. c), d.lgs. 196/2003	Artt. 26, 28, 29, 35, comma 1, lett. a), d.lgs. 165/2001.	Personali, sensibili, giudiziari	Raccolta, Registrazione Organizzazione Conservazione Consultazione Elaborazione Selezione Estrazione Raffronto Utilizzo Blocco Cancellazione Distruzione
Selezione	Art. 112, comma 1e 2, lettere a) e c), d.lgs. 196/2003	Artt. 35, comma 1, lett. b) e 39 d.lgs. 165/2001.	Personali, sensibili, giudiziari	Raccolta, Registrazione Organizzazione Conservazione Consultazione Elaborazione Selezione Estrazione Raffronto Utilizzo Blocco Cancellazione Distruzione

Tab. 13

COSTITUZIONE RAPPORTO DI LAVORO				
Attività	**Finalità rilevante interesse pubblico**	**Fonte legislativa**	**Tipologia dati**	**Operazioni eseguibili**
Stipulazione rapporto di lavoro	Art. 112, comma 1 d.lgs. 196/2003	Artt. 2, comma 2, 7, comma 6, 36, comma 1, d.lgs. 165/2001- CCNL	Personali e sensibili	Raccolta, Registrazione Organizzazione Conservazione Consultazione Elaborazione Selezione Estrazione Raffronto Comunicazione Utilizzo Blocco Cancellazione Distruzione

Tab. 14

RAPPORTO DI LAVORO				
Attività	**Finalità rilevante interesse pubblico**	**Fonte legislativa**	**Tipologia dati**	**Operazioni eseguibili**
Inquadramento	Art. 112, comma 2, lett. d) d.lgs. 196/2003	Art. 52 d.lgs. 165/2001 - CCNL	Personali	Raccolta, Registrazione Organizzazione Conservazione Consultazione Elaborazione Selezione Estrazione Raffronto Comunicazione Utilizzo Blocco Cancellazione Distruzione
Attribuzioni trattamento economico		Artt. 2, comma 2, 24, 45 d.lgs. 165/2001; CCNL d.lgs. 151/2001	Personali e sensibili	Idem c.s.
Cessione quinto stipendio	Art. 68, comma 1, d.lgs. 196/2003	Art. 33 Dpr 3/1957	Sensibili	Idem c.s.
Contributi (invalidità, vecchiaia, superstiti)	Art. 112, comma 2, lett. f) d.lgs. 196/2003	L. 335/1995; Dpr 1092/1973; d.lgs. 503/1992; d.lgs. 151/2001	Personali e sensibili	Idem c.s. Comunicazione INDAP
Assicurazione	Art. 112, comma 2, lett. b) d.lgs. 196/2003	Artt. 1, 4, 9 Dpr 1124/1965	Personali e sensibili	Idem c.s. e Comunicazione INAIL
Obblighi fiscali	Art. 112, comma 2, lett. d) d.lgs. 196/2003	Art. 1 Dpr 600/1973	Personali e sensibili	Idem c.s. e Comunicazione al Ministero economia e Finanze
Pari opportunità	Art. 112, comma 2, lett. b) d.lgs. 196/2003	Artt. 7, comma 1, 57 d.lgs. 165/2001; CCNL	Personali e sensibili	Idem c.s.
Formazione	Art. 112, comma 1, d.lgs. 196/2003	Artt. 7, comma 4, 7 *bis* d.lgs. 165/2001	Personali e sensibili	Idem c.s
Valutazione	Art. 112, comma 1, d.lgs. 196/2003	Artt. 20, 21 d.lgs. 165/2001	Personali e sensibili	Idem c.s e Modificazione

Tav. 15

RAPPORTO DI LAVORO (Segue)				
Attività	**Finalità rilevante interesse pubblico**	**Fonte legislativa**	**Tipologia dati**	**Operazioni eseguibili**
Assenza per malattia	Art. 112, comma 1, d.lgs. 196/2003	Art. 2, comma 2, d.lgs. 165/2001; CCNL	Personali e sensibili	Raccolta, Registrazione Organizzazione Conservazione Consultazione Elaborazione Selezione Estrazione Raffronto Comunicazione Utilizzo Blocco Cancellazione Distruzione
Mutamento mansioni per inidoneità psicofisica	Art. 112, comma 1, d.lgs. 196/2003	CCNL	Personali e sensibili	Idem c.s.
Permessi e congedi parentali	Art. 112, comma 1, d.lgs. 196/2003	Art. 23 d.lgs. 165/2001	Personali e sensibili	Idem c.s.
Congedo per maternità	Art. 112, comma 1, d.lgs. 196/2003	L. 1204/1971; d.lgs. 151/2001; CCNL	Personali e sensibili	Idem c.s.
Diritto allo studio	Art. 112, comma 1, d.lgs. 196/2003	Art. 10 Statuto lav. ; art. 5 L. 53/2000	Personali e sensibili	Idem c.s.
Aspettative: sindacali motivi personali/familiari attività extraimpiego cariche pubbliche elettive dottorato ricerca coniuge all'estero cooperazione paesi in via di sviluppo, impiego presso O.I. e stati esteri	Art. 42 d.lgs. 165/2001 Statuto lav CCNL Art. 68 d.lgs. 165/2001 Art. 2 L. 476/1984 L. 26/1980 L. 114/1962 Art. 23 d.lgs. 165/2001	d.lgs. 165/2001; CCNL	Personali e sensibili	Idem c.s.
Infortunio sul lavoro	Art. 112, comma 2, lett. f) d.lgs. 196/2003	Art. 9 Dpr 1124/1965	Personali e sensibili	Idem c.s. e Comunicazione a INAIL e PS ex artt. 53 e 54 Dpr 1124/1965
Malattie professionali	Art. 112, comma 2, lett. d) d.lgs. 196/2003	Art. 51, comma 2, d.lgs. 165/2001; Statuto lav.; CCNL	Personali e sensibili	Idem c.s.
Igiene e sicurezza sul lavoro	Art. 112, comma 2, lett. i) d.lgs. 196/2003	D.lgs. 626/1994; d.lgs. 151/2001	Personali e sensibili	Idem c.s.
Esercizio diritti sindacali	Art. 112, comma 2, lett. e) d.lgs. 196/2003	Artt. 9 e 50 d.lgs. 165/2001; CCNL	Personali e sensibili	Idem c.s.
Procedimenti disciplinari	Art. 112, comma 2, lett. c) d.lgs. 196/2003	Art. 2, comma 2, 55 d.lgs. 165/2001; CCNL	Personali, sensibili e giudiziari	Idem c.s. e Modificazioni
Incompatibilità	Art. 112, comma 2, lett. l) e m) d.lgs. 196/2003	Art. 53 d.lgs. 165/2001	Personali e sensibili	Idem c.s.
Trasferimenti	Art. 112, comma 2, lett. c) d.lgs. 196/2003	Art. 2, comma 2, d.lgs. 165/2001; CCNL	Personali	Idem c.s.

Tav. 16

MOBILITA'				
Attività	**Finalità rilevante interesse pubblico**	**Fonte legislativa**	**Tipologia dati**	**Operazioni eseguibili**
Passaggio personale tra PA diverse	Art. 112, comma 1, d.lgs. 196/2003	Art. 30 d.lgs. 165/2001	Personali e sensibili	Raccolta, Registrazione Organizzazione Conservazione Consultazione Elaborazione Selezione Estrazione Raffronto Comunicazione Utilizzo Blocco Cancellazione Distruzione
Passaggio per trasferimento attività	Art. 112, comma 1, d.lgs. 196/2003	Art. 31 d.lgs. 165/2001	Personali e sensibili	Idem c.s.
Eccedenza di personale e mobilità collettiva	Art. 112, comma 1, d.lgs. 196/2003	Art. 33 d.lgs. 165/2001	Personali e sensibili	Idem c.s.

Tav. 17

ESTINZIONE RAPPORTO DI LAVORO				
Attività	**Finalità rilevante interesse pubblico**	**Fonte legislativa**	**Tipologia dati**	**Operazioni eseguibili**
Dimissioni con / senza preavviso	Art. 112, comma 1,lett. c), d.lgs. 196/2003	Art. 2 d.lgs. 165/2001; CCNL	Personali	Raccolta, Registrazione Organizzazione Conservazione Consultazione Elaborazione Selezione Estrazione Raffronto Comunicazione Utilizzo Blocco Cancellazione Distruzione
Cessazione impiego per sopraggiunti motivi d'età	Art. 112, comma 1, lett. c), d.lgs. 196/2003	Art. 2, comma 21, L. 335/95; art. 16 d.lgs. 503/1992	Personali e sensibili	Idem c.s.
Recesso dell'Amministrazione	Art. 112, comma 1, lett. c), d.lgs. 196/2003	Art. 33 d.lgs. 165/2001	Personali e sensibili	Idem c.s

Tab. 18

TRATTAMENTO FINE RAPPORTO				
Attività	**Finalità rilevante interesse pubblico**	**Fonte legislativa**	**Tipologia dati**	**Operazioni eseguibili**
Buonuscita	Art. 112, comma 1, lett. f), d.lgs. 196/2003	Dpr 1032/1973	Personali e sensibili	Raccolta Registrazione Organizzazione Conservazione Consultazione Elaborazione Selezione Estrazione Raffronto Utilizzo Blocco Cancellazione Distruzione e Comunicazione a INDAP
TFR	Art. 112, comma 1, lett. f), d.lgs. 196/2003	L. 335/1995	Personali e sensibili	Idem. c.s .e Comunicazione a INDAP

Tab. 19

ORGANI				
Attività	**Finalità rilevante interesse pubblico**	**Fonte legislativa**	**Tipologia dati**	**Operazioni eseguibili**
Insediamento	Art. 112 d.lgs. 196/2003	l.r. 40/2005 e ss.mm.	Personali e sensibili	Raccolta Registrazione Organizzazione Conservazione Consultazione Elaborazione Selezione Estrazione Raffronto Utilizzo Blocco Cancellazione Distruzione
Altri incarichi ricoperti	Art. 112 d.lgs. 196/2003	8 febbraio 2008, n. 5	Personali e sensibili	Idem c.s.
Pagamento indennità	Art. 112 d.lgs. 196/2003	l.r. 40/2005 e ss.mm.	Personali e sensibili	Idem c.s.
Stato patrimoniale	Art. 112 d.lgs. 196/2003	l.r. 5/2008	Personali e sensibili	Idem c.s.
Dimissioni	Art. 112 d.lgs. 196/2003	l.r. 40/2005 e ss.mm.	Personali e sensibili	Idem c.s
Decadenza	Art. 112 d.lgs. 196/2003	l.r. 40/2005 e ss.mm.	Personali e sensibili	Idem c.s

3.4.3 Adempimenti di ARS nel caso di aggiudicazione a terzi di servizi, forniture, beni.

Ogni qualvolta si proceda ad aggiudicazione a terzi di servizi, forniture e beni, è opportuno far compilare al terzo la clausola di garanzia di cui ***all'Allegato 6,*** ove sono previste forme di garanzia e regole cui i terzi dovranno informarsi.

Trattativa privata: le garanzie previste dalla normativa sulla privacy devono essere esplicitate anche all'interno dei modelli standard utilizzati per l'affidamento, in particolare si fa riferimento al modello per l'inserimento nell'elenco fornitori, ***Allegato 15.***
Qualora fosse pubblicato un avviso di trattativa privata si rende opportuno inserire la seguente formula: "*TUTELA PRIVACY*
Ai sensi dell' art. 10 della d.lgs. 196/03 si comunica che i dati personali relativi alle imprese partecipanti alla trattativa privata saranno oggetto di trattamento con o senza ausilio di mezzi elettronici limitatamente e per il tempo necessario alla trattativa privata.
Sono fatti salvi i diritti che l'art. 7 del d.lgs. 196/2003 garantisce ai soggetti interessati.
Il Responsabile del trattamento dei dati personali è individuato nella persona del Direttore di ARS, Dott.ssa Laura Tramonti, Via Vittorio Emanuele II, n. 64 – 50134-Firenze, fax 055/4624330, e-mail: laura.tramonti@arsanita.toscana.it".
Nel capitolato generale e speciale, nonché all'interno del contratto, è opportuno inserire una formula di garanzia sulla privacy, secondo l'esempio seguente: "*TUTELA PRIVACY*
I dati forniti dagli offerenti in occasione della partecipazione alla presente gara saranno trattati esclusivamente ai fini della gara stessa e della successiva eventuale stipula del contratto, ai sensi dell'art. 18 del d.lgs. n. 196/2003, compatibilmente con le funzioni istituzionali, le disposizioni di legge e regolamentari concernenti i pubblici appalti e le disposizioni riguardanti il diritto di accesso ai documenti ed alle informazioni.
Sono fatti salvi i diritti che l'art. 7 del d.lgs. 196/2003 garantisce ai soggetti interessati.
Il Responsabile del trattamento dei dati personali è individuato nella persona del Direttore di ARS, Dott.ssa Laura Tramonti, Via Vittorio Emanuele II, n. 64 – 50134-Firenze, fax 055/4624330, , e-mail: laura.tramonti@arsanita.toscana.it".

3.4.3.1 Casi specifici

Si giunge alla stipula del contratto con soggetti terzi in esito di uno specifico procedimento amministrativo, a formazione progressiva così cronologicamente e logicamente strutturato: indagine commerciale, individuazione contraente; richiesta di offerta; sottoscrizione del contratto; esecuzione dello stesso.

Indagine commerciale:
Tale fase è finalizzata ad ottenere tutte le informazioni necessarie relative ai futuri contraenti circa la qualità, il prezzo, i tempi di fornitura e/o consegna dei beni e/o

servizi, calibrate sullo specifico interesse dell'Agenzia. In questa fase tuttavia, non rilevano dati sensibili, né personali.

Individuazione del contraente

I risultati dell'indagine commerciale, sussunti in una relazione, costituiscono la base su cui l'amministrazione maturerà la scelta del futuro contraente. Visto che la scelta, per la procedura in oggetto si incentra esclusivamente sulle caratteristiche dei beni e servizi, prescindendo da indagini afferenti ai soggetti contraenti, non rilevano dati sensibili.

Richiesta offerta

Una volta individuato il contraente che offre beni e/o servizi che sono conformi all'interesse della amministrazione, quest'ultima avvia l'istruttoria circa il soggetto contraente. Nel verificare lo stato patrimoniale della società, attraverso visure camerali, acquisendo i dati relativi ai legali rappresentanti dei futuri contraenti, attraverso la sottoscrizione dei preventivi con firma autenticata , quindi con l'inoltro della loro carta di identità, inizia il trattamento di dati sensibili, ragion per cui dovranno essere adottate le tutele previste dal Codice, secondo quanto prescritto nel presente documento per ciò che concerne le prescrizioni generali e nel paragrafo successivo relativamente alle istruzioni specifiche correlate la profilo di autorizzazione.

Aggiudicazione e sottoscrizione del contratto

A seguito della fase precedente i dati sensibili acquisiti continuano ad essere trattati anche nelle successive fasi del rapporto contrattuale, per cui dovranno essere osservate le prescrizioni imposte dalla normativa sulla privacy.

Riassumendo:

Tab. 20 – Stipula del contratto – Sintesi procedimento amministrativo

Attività	Finalità rilevante interesse pubblico	Fonte legislativa	Tipologia dati	Operazioni eseguibili
Indagine commerciale	Art. 19 d.lgs. n. 196/2003 e relative disposizioni attuative l.r. 38/2007 e relativo regolamento di attuazione	**L. 241/1990 come modificata dalla L. 15/2005; L. 20 marzo 1865 n. 2248 All. F; L. 205/2000d.lgs. 157/1995; Direttiva 2004/18/CE, nuovo Codice dei contratti pubblici**	**Comuni**	Raccolta, Registrazione Organizzazione Conservazione Consultazione Elaborazione Selezione Estrazione Raffronto Comunicazione Utilizzo Blocco Cancellazione Distruzione
Individuazione del contraente	Art. 19 d.lgs. n. 196/2003 e relative disposizioni attuative l.r. 38/2007 e relativo regolamento di attuazione	**Idem come sopra**	**Comuni**	Idem c.s.
Richiesta offerta	Art. 20, 21, 22 d.lgs. n. 196/2003 e relative disposizioni attuative l.r. 38/2007 e relativo regolamento di attuazione	**Idem come sopra**	**Sensibili , giudiziari e comuni**	Idem c.s.
Aggiudicazione	Art. 20 d.lgs. n. 196/2003 e relative disposizioni attuative l.r. 38/2007 e relativo regolamento di attuazione	**Idem come sopra**	**Sensibili e comuni**	Idem c.s.
Sottoscrizione del contratto	Art. 20 d.lgs. n. 196/2003 e relative disposizioni attuative l.r. 38/2007 e relativo regolamento di attuazione	**Idem come sopra**	**Sensibili e comuni**	Idem c.s.

3.4.4 Adempimenti relativi ai fornitori che possono venire a conoscenza di dati personali

Per garantire che il personale di ditte fornitrici, che si trovi ad intervenire presso l'amministrazione dell'Agenzia, o che operi nell'ambito di forniture che trattino qualsiasi tipologia di dati personali, operi nel rispetto delle disposizioni in materia di protezione dei dati personali, gli incaricati adottano le seguenti idonee misure:

- ✓ deve essere fatta esplicita e formale richiesta al fornitore già nominato dal Titolare Responsabile esterno, di redazione di opportuno rapporto di intervento ogni qual volta questo sia dovuto, da redigere con modalità conformi alla vigente normativa, che dovrà essere controfirmato da un rappresentante del Settore/Ufficio competente all'atto della consegna;, (es.: il Titolare che nell'implementare le misure di sicurezza si avvale di soggetti esterni all'Agenzia; o nel caso in cui, procedendo all'aggiornamento dei sistemi informatici, s'intenda avvalersi del supporto di soggetti esterni all'Ente);
- ✓ il fornitore dovrà indicare, al settore/ufficio competente, il personale incaricato del trattamento ed impegnarsi ad eseguire il medesimo con i limiti e le garanzie del Codice, nonché delle disposizioni emanate in materia dall'ARS (valgono al riguardo le considerazioni svolte al precedente punto 3.4.3 in merito alle clausole di garanzia);
- ✓ qualora i soggetti interessati cessino di svolgere, definitivamente o comunque per un periodo superiore a sei mesi, le funzioni per le quali hanno ricevuto l'incarico, dovrà essere data tempestiva comunicazione al Gruppo privacy che provvederà a revocare il diritto di accesso ai locali ed ai sistemi.

3.4.5 Il contenzioso.

Nell'espletamento dell'attività amministrativa di ARS occorre annoverare anche l'attività di gestione del contenzioso sebbene, almeno fino ad oggi, ha riguardato solo marginalmente l'attività degli uffici.
Occorre preliminarmente distinguere tra attività stragiudiziale e giudiziale:

- ✓ la prima è destinata ad esaurirsi in seno all'Agenzia e pertanto, sotto il profilo della tutela della riservatezza, deve essere disciplinata in ogni sua fase;
- ✓ la seconda, quella giudiziale appunto, comporta la trasmissione di atti contenenti dati sensibili e/o giudiziari da ARS a altro ente pubblico (l'Avvocatura regionale) o a soggetto privato (studio legale esterno).

Seguono le ***Tabelle 21 e 22*** riassuntive delle attività di competenza della struttura tecnico-amministrativa della Direzione, inerenti il contenzioso, con indicazione delle fonti legislative di riferimento, della tipologia dei dati e delle operazioni eseguibili.

Tab. 21

CONTENZIOSO STRAGIUDIZIALE				
Attività	**Finalità rilevante interesse pubblico**	**Fonte legislativa**	**Tipologia dati**	**Operazioni eseguibili**
Ricezione ricorso	Art. 20, 21, 22 d.lgs. n. 196/2003	L. 241/1990 come modificata dalla L. 15/2005;	Sensibili e giudiziari	Raccolta Registrazione
Comunicazione al CDA Comunicazione interessati	Art. 20, 21, 22 d.lgs. n. 196/2003	L. 241/1990 come modificata dalla L. 15/2005	Sensibili e giudiziari	Comunicazione
Istruttoria	Art. 20, 21, 22 d.lgs. n. 196/2003	L. 241/1990 come modificata dalla L. 15/2005	Sensibili e giudiziari	Registrazione Organizzazione Conservazione Consultazione Elaborazione Selezione Estrazione Raffronto Utilizzo
Acquisizione informazioni e/o documenti presso altri enti	Art. 20, 21, 22 d.lgs. n. 196/2003	L. 241/1990 come modificata dalla L. 15/2005 l.r. 2 dicembre 2005, n. 63	Sensibili e giudiziari	Idem c.s.
Redazione risposta	Art. 20, 21, 22 d.lgs. n. 196/2003	L. 241/1990 come modificata dalla L. 15/2005	Sensibili e giudiziari	Idem c.s.
Comunicazione a CDA Comunicazione interessati	Art. 20, 21, 22 d.lgs. n. 196/2003	L. 241/1990 come modificata dalla L. 15/2005	Sensibili e giudiziari	Comunicazione
Conservazione fascicolo	Art. 20, 21, 22 d.lgs. n. 196/2003	l.r. 2 dicembre 2005, n. 63	Sensibili e giudiziari	Conservazione Blocco Cancellazione Distruzione

Tab. 22

CONTENZIOSO GIUDIZIALE				
Attività	**Finalità rilevante interesse pubblico**	**Fonte legislativa**	**Tipologia dati**	**Tipologia trattamento**
Ricezione ricorso	Art. 20, 21, 22 d.lgs. n. 196/2003	L. 241/1990 come modificata dalla L. 15/2005; l.r. 2 dicembre 2005, n. 63	Sensibili Giudiziari	Raccolta
Comunicazione al CDA	Art. 20, 21, 22 d.lgs. n. 196/2003	L. 241/1990 come modificata dalla L. 15/2005; l.r. 2 dicembre 2005, n. 63	Sensibili Giudiziari	Comunicazione
Istruttoria/Predisposizione relazione	Art. 20, 21, 22 d.lgs. n. 196/2003	L. 241/1990 come modificata dalla L. 15/2005 l.r. 2 dicembre 2005, n. 63	Sensibili Giudiziari	Registrazione Organizzazione Conservazione Consultazione Elaborazione Selezione Estrazione Raffronto Utilizzo
Trasmissione ricorso e risultanze istruttorie alla Avvocatura regionale[49]	Art. 20, 21, 22 d.lgs. n. 196/2003	L. 241/1990 come modificata dalla L. 15/2005 l.r. 2 dicembre 2005, n. 63	Sensibili Giudiziari	Comunicazione
Trasmissione ricorso e risultanze istruttorie a Studio legale esterno[50]	Art. 20, 21, 22 d.lgs. n. 196/2003	L. 241/1990 come modificata dalla L. 15/2005 l.r. 2 dicembre 2005, n. 63	Sensibili Giudiziari	Raccolta e comunicazione

[49] La trasmissione del contenzioso all'Avvocatura regionale avviene ai sensi della l.r. 2 Dicembre 2005, n. 63.

[50] Ai sensi della l.r. n. 63/2005 ARS può farsi rappresentare e difendere in giudizio avvalendosi di uno studio legale esterno, soltanto nei casi di incompatibilità, carico di lavoro dell'Avvocatura regionale, motivata opportunità; in questi tassativi casi, la procedura per la comunicazione dei dati avviene secondo le disposizioni dettate in materia di comunicazione da soggetto pubblico a privato. Si rinvia, pertanto, al §. 2.3.5.2. "*Comunicazione dati personali da soggetto a soggetto pubblico o soggetto privato"*.

3.4.6. Diritto di accesso e privacy

Il rapporto tra l'attività della pubblica amministrazione e la privacy è divenuto sempre più conflittuale da quando il legislatore – dapprima con la legge n. 142 del 1990 e, poi, con legge n. 241 del 1990 – ha aperto le porte delle amministrazioni pubbliche agli amministrati garantendo loro il diritto d'accesso ai documenti amministrativi.
Il nuovo Codice ha ridisegnato il quadro legislativo relativo alle amministrazioni pubbliche. Anzitutto, nella Parte I, Titolo III, Capo II (artt. 18- 22), dove declina, in rapida progressione, una serie di regole specifiche che tutti i soggetti pubblici devono osservare nel trattamento dei dati; nella Parte II, Titolo IV (artt. 59-74) regolamenta il trattamento dei dati in ambito pubblico, iniziando con la spinosa problematica relativa all'accesso ad atti ed informazioni in possesso dell'amministrazione.
I diritti di accesso di cui all'art. 7 del Codice possono essere fatti valere nei confronti del proprio datore di lavoro, qualora il prestatore di lavoro inoltri una richiesta di accesso ai sensi dell'art. 7, il datore è tenuto, come ogni altro titolare, ad indicare tutte le informazioni comuni e sensibili in suo possesso relative al dipendente, ivi comprese le c.d. note di qualifica.

Analizziamo le singole fattispecie che possono realizzarsi nel rapporto tra accesso a atti amministrativi e privacy:
a) accesso a documenti amministrativi
b) accesso a dati personali
c) accesso ai propri dati personali;
d) accesso a dati personali di terzi.

Nel caso sub. lett. a) "Accesso ai documenti amministrativi", occorre in via preliminare, precisare che sia la giurisprudenza che il Garante hanno più volte affermato che la legge di tutela sulla privacy non può essere presa a pretesto per negare l'accesso agli atti amministrativi.
Cominciamo con l'analizzare l'art. 59[51] del Codice, il quale prevede che *l'accesso ai documenti amministrativi* sia regolato dalla legge n. 241/1990 per cui, nel caso di accesso a documento amministrativo contenente i dati del richiedente l'accesso, trova applicazione l'art. 24 della legge n. 241/90 e l'art. 7 sarebbe per così dire limitato a regolare i casi in cui emergono dati personali del richiedente non sussulti in un atto amministrativo.
Del resto lo stesso art. 22 della legge n. 241/90, così come di recente modificato dalla legge n. 15/2005, prevede che siano accessibili nella pubblica amministrazione solo quelle informazioni che assumono la veste di documento amministrativo.
In conseguenza a quanto affermato fino a questo punto possiamo agilmente affermare che per individuare quale sia la norma da applicare al caso concreto, di fronte ad una richiesta d'accesso occorre preliminarmente individuare l'oggetto della richiesta;

[51] **59. Accesso a documenti amministrativi.**
1. Fatto salvo quanto previsto dall'articolo 60, i presupposti, le modalità, i limiti per l'esercizio del diritto di accesso a documenti amministrativi contenenti dati personali, e la relativa tutela giurisdizionale, restano disciplinati dalla legge 7 agosto 1990, n. 241, e successive modificazioni e dalle altre disposizioni di legge in materia, nonché dai relativi regolamenti di attuazione, anche per ciò che concerne i tipi di dati sensibili e giudiziari e le operazioni di trattamento eseguibili in esecuzione di una richiesta di accesso. Le attività finalizzate all'applicazione di tale disciplina si considerano di rilevante interesse pubblico.

successivamente, se sono dati personali, troverà applicazione il Codice privacy, mentre se trattasi di documenti amministrativi si applicherà la legge n. 241/90.
Per ARS oltre alla legge 241/90 deve farsi riferimento ai seguenti atti legislativi e d'indirizzo regionali:

- **l.r. 9/95** "*Disposizioni in materia di procedimento amministrativo e di accesso agli atti";*
- **Deliberazione Giunta regionale n. 612 del 2.6.1997** *"l.r. 9/95: Disposizioni in materia di procedimento amministrativo e di accesso agli atti – art. 51 – Limitazione al diritto di accesso";*
- **Deliberazione Giunta regionale n. 1307 del 2/11/1998** *"Direttiva in ordine all'accesso ed alla conoscenza dei documenti amministrativi della Regione Toscana (pubblicata sul supplemento straordinario al BURT n. 49/98).*

Nel caso sub. lett. b) quando l'accesso riguarda specificatamente i dati sensibili valgono le seguente considerazioni.
In caso di documenti che contengono dati sensibili si raccomanda di valutare con attenzione la legittimazione del richiedente. In questo caso, infatti, il soggetto richiedente è legittimato all'accesso, solo qualora l'accesso dell'atto gli sia necessario per difendere in giudizio i propri diritti e interessi.
Resta ferma il principio per cui i conflitti tra diritto di accesso e riservatezza dei terzi devono essere risolti nel senso che l'accesso, finalizzato per la cura e la difesa di propri interessi legittimi, prevale rispetto all'esigenza di riservatezza nei limiti però in cui esso è necessario alla difesa di un interesse giuridicamente rilevante.
Dati super sensibili *(dati idonei a rilevare lo stato di salute e la vita sessuale)*
L'art. 60[52] del Codice fornisce la disciplina per il trattamento di dati idonei a rivelare lo stato di salute o la vita sessuale, dati cc.dd "*supersensibili"* pone una disciplina più rigida di quella prevista dall'art. 59 **e consente il loro trattamento solo se la situazione che si vorrebbe tutelare con la richiesta di accesso sia di rango almeno pari ai diritti dell'interessato, ovvero consista in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile.**

[52] **Art. 60. Dati idonei a rivelare lo stato di salute e la vita sessuale.**
1. Quando il trattamento concerne dati idonei a rivelare lo stato di salute o la vita sessuale, il trattamento è consentito se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso ai documenti amministrativi è di rango almeno pari ai diritti dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile.

Nel caso sub c) accesso ai propri dati personali, trova applicazione l'art. 7[53] del Codice che attribuisce all'interessato il potere di ottenere comunicazione dei propri dati personali in forma intellegibile, mediante la procedura prevista dai successivi articoli 8 e seguenti: la richiesta va rivolta senza formalità al titolare o al responsabile (art. 8); l'istanza può essere trasmessa anche mediante lettera raccomandata, telefax o posta elettronica e può essere formulata anche oralmente (art. 9). Si veda al riguardo il fac-simile ***Allegato 16***. A sua volta, il responsabile può comunicare i dati all'interessato oralmente, oppure mediante strumenti elettronici (art. 10).
L'interessato può, altresì, esercitare il diritto di accesso al registro dei trattamenti tenuti dal Garante per la protezione dei dati personali, rivolgendo istanza al fine di conoscere, mediante accesso gratuito al registro di cui all'art. 154, comma 1, lett. l) del d.lgs. 196/2003, l'esistenza di trattamenti di dati che possono riguardarlo.
Ai fini predetti deve specificare una o più delle seguenti opzioni: peculiarità del proprio lavoro, famiglia, stato civile, attività effettuate, appartenenza a circoli, corrispondenza intrattenute con Enti/Aziende, mezzi di trasporto utilizzati, acquisti etc., dalle quali si possa rilevare l'ambito di trattamenti che possono essere rilevanti ai fini della tutela dei propri interessi legittimi).
I diritti riferiti ai dati personali di persone decedute possono essere esercitati da chiunque abbia interesse dimostrabile.
Nell'esercizio dei diritti l'interessato può dare delega o procura scritta persone fisiche o associazioni. In tal caso la circostanza deve essere esplicitata ed è preferibile allegare fotocopia dell'atto stesso. ***(cfr. Modello Fac-Simile Allegato 17).***

L'esercizio del diritto di accesso ai propri dati personali incontra più limiti quando l'istanza è rivolta ad una struttura sanitaria. In questi casi, l'art. 84, comma 1, del Codice, precisa che la comunicazione deve avvenire solo per il tramite di un medico designato dall'interessato o dall'organizzazione sanitaria.
Bisogna però tener presente la circostanza che il Codice (agli artt. 7 e ss.) fa riferimento a «dati personali» e non a «documenti amministrativi». Naturalmente, i

---

[53] **Art. 7. Diritto di accesso ai dati personali ed altri diritti.**
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.

dati personali sono spesso contenuti anche in atti e documenti amministrativi ma, a ben vedere, l'art. 7 regolamenta solo il diritto di accesso alle informazioni di carattere personale relative all'interessato e non anche il diritto di accesso ad atti e documenti amministrativi.

Nel caso sub d) accesso ai dati di terzi valgono le seguenti considerazioni.
Se volessimo ricercare un criterio indicativo per regolare il rapporto tra accesso e privacy, potremmo affermare che la normativa sulla privacy non avendo abrogato il regime di pubblicità degli atti delle pubbliche amministrazioni abbia riconosciuto la prevalenza del diritto di accesso rispetto al diritto alla riservatezza (almeno quando si tratta di accedere a documenti contenenti dati personali comuni).
Esistono, tuttavia, alcuni limiti che incontra il diritto di accesso davanti alla tutela della riservatezza e cioè, quello relativo all'esigenza superiore di tutelare la riservatezza di terzi, persone, gruppi ed imprese, tutela che però che si comprime solo di fronte al diritto di accesso funzionale a difendere i propri interessi giuridici.
Anche con la nuova legge n. 15/2005 la prevalenza è accordata al diritto d'accesso, dato che la stessa non si limita più a garantire solo la mera visione degli atti, ma si spinge fino ad assicurare all'interessato anche la possibilità di estrarre copia dei documenti amministrativi.

3.4.6.1 Diritto di accesso degli Organi di ARS e degli Organi regionali

Gli Organi di ARS e gli Organi regionali hanno diritto di ottenere tutte le informazioni in possesso degli uffici che siano utile all'espletamento del loro mandato.
La concreta individuazione da parte degli uffici delle notizie ed informazioni che possono essere comunicate deve tenere conto di tutto ciò che può essere funzionale allo svolgimento del mandato e, quindi, consentire di valutare con piena cognizione di causa l'operato dell'Amministrazione, di esprimere un giudizio consapevole sulle questioni sottoposte agli stessi Organi e promuovere le iniziative di rispettiva competenza.

3.4.7 Profili e relative istruzioni

Il paragrafo affronta nello specifico le istruzioni da impartire agli incaricati del trattamento della struttura tecnico-amministrative assegnate alla Direzione

La metodologia di lavoro adottata e le disposizioni a cui attenersi sono funzione del profilo assegnato all'incaricato:

3.4.7.1 Amministratore banca dati specifica F

Questo profilo viene assegnato agli sviluppatori e/o responsabili della gestione e manutenzione di banche dati contenenti dati sensibili inerenti la gestione del personale e le attività contrattuali *(Vedi § 3.4 - Tabella delle Attività da 11 a 22).*

Gli incaricati a cui è assegnato questo profilo dovranno attenersi alle seguenti istruzioni specifiche in relazione alle operazioni di seguito identificate:

- *Comunicazione al Gruppo Privacy*

Ogni Amministratore di banca dati è tenuto a dare comunicazione al Referente del Gruppo Privacy della creazione della banca dati; devono inoltre essere indicati: l'ubicazione della banca, una descrizione breve dei dati contenuti, della provenienza e l'elenco degli utenti incaricati. Deve essere inoltre tempestivamente comunicata ogni variazione di dette informazioni.

- *Separazione e Cifratura*

E' compito di questo profilo gestire la banca dati in oggetto adottando le tecniche informatiche utili per il rispetto della normativa Privacy.
Ogni archivio presente nella banca dati in oggetto deve essere organizzato in modo tale da garantire la separazione tra i dati personali e i dati sulla salute dati comuni e dati sensibili.
L'interconnessione viene resa disponibile solo per il tempo necessario al trattamento.
Ai fini dell'analisi statistica sui soggetti, le entità contenenti i soli dati sulla salute possono includere degli identificativi personali opportunamente criptati per mezzo di algoritmi di cifratura a chiave segreta.
E' compito di questo profilo criptare i dati suddetti e custodire la chiave segreta di decriptazione.

- *Supporto fisico degli archivi*

Gli archivi, che contengono dati sensibili devono essere riposti, ogni volta che si è terminato il trattamento o comunque alla fine della giornata di lavoro, in cartelle criptate sul file-server centrale.
Per creare una cartella criptata occorre spostarsi sulla propria cartella di DocServer, creare una nuova cartella, ciccare sulla stessa con il tasto destro, scegliere proprietà e nel Tab "*generale*" cliccare sul pulsante "*avanzate*" e spuntare la voce "*crittografa contenuto per la protezione dei dati*".

3.4.7.2 Operatore inserimento Dati G

Questo profilo viene assegnato agli operatori delle banche dati specifiche che devono svolgere attività di inserimento dati.
Gli incaricati con questo profilo hanno accesso alle banche dati solo per fare modifiche e/o nuovi inserimenti dati.

- *Modalità di accesso*

L'accesso alla banca dati specifica viene gestito dagli incaricati con profilo C;
Il profilo in oggetto non è autorizzato a eseguire elaborazioni o estrazioni dall'archivio ma solo ad apportare modifiche o eseguire nuovi inserimenti.

3.4.7.3 Operatore segreteria H

Questo profilo viene assegnato al personale addetto alla segreteria, al protocollo, alla logistica, reception e servizio pulizie. Qualora nell'ambito dello svolgimento dei propri compiti,) il personale in oggetto prenda visione di dati sensibili si raccomanda il pieno rispetto delle prescrizioni generali e dei principi del codice in materia di dati sensibili. In particolare:

- **Gestione del protocollo**

Nell'ambito dell'attività è necessario archiviare solo le porzioni di informazione non sensibile provvedendo all'occultamento o all'omissione di eventuali allegati contenente informazioni sensibili.

- **Invio richiesta dati sensibili**

Qualora nell'ambito dell'attività si debba richiedere a soggetti/enti esterni ad ARS documenti contenenti dati sensibili è necessario allegare alla richiesta la formulazione di cui all'allegato (4/B).

Inoltre occorre indicare a soggetti/enti suddetti le modalità per la trasmissione dei dati in oggetto al fine di garantire la tutela della riservatezza dei dati inviati.
Le modalità di trasmissione ammesse sono:

- ✓ posta ordinaria in busta chiusa con dizione "Riservato" e nominativo del destinatario;
- ✓ Consegne manuali;
- ✓ trasmissione criptata di dati;
- ✓ ax con indicazione del destinatario.

Si ricorda che tale attività è limitata ai dati in entrata, mentre è fatto assoluto divieto di trasmissione all'esterno di dati sensibili se non preventivamente autorizzata dal Responsabile del trattamento.

ALLEGATI

INDICE ALLEGATI

ALLEGATO 12	*REGISTRO CONVENZIONI/PROTOCOLLI D'INTESA/CONTRATTI STIPULATI CON ALTRI ENTI AI FINI DELL'ACCESSO DA PARTE DI ARS AI FLUSSI DI DATI ATTINENTI ALLA SALUTE O PER L'ACCESSO DA PARTE DI DI ALTRI ENTI AI DATI DI ARS*
ALLEGATO 13	*PORTALE PRIVACY*
ALLEGATO 14	*FAC-SIMILE DETERMINE DIRETTORE/COORDINATORI NOMINA INCARICATI DEL TRATTAMENTO*
ALLEGATO 15	*FAC-SIMILE RICHIESTA DITTA INSERIMENTO ELENCO FORNITORI ARS*
ALLEGATO 16	*FAC-SIMILE ESERCIZIO DIRITTI DELL'INTERESSATO*
ALLEGATO 17	*FAC-SIMILE ACCESSO AL REGISTRO DEI TRATTAMENTI TENUTI DAL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI*