DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

ALLEGATO N. 8

Lettera di incarico – Istruzioni per gli incaricati

(DECRETO LEGISLATIVO 30 GIUGNO 2003, n. 196)

TITOLARE DEI DATI: COMUNE DI ANCONA

RIF : D.G 112 del 26.03.2008 e succ. Mod.

LETTERA DI INCARICO
- articolo 30 del d. lgs. 196/2003 (codice della privacy) -

Con la presente, il sottoscritto, in qualità di responsabile del trattamento, comunica che la S.V. **è preposta come incaricato, ai sensi dell'art. 30 del codice della privacy, allo svolgimento di operazioni di trattamento necessarie e strumentali allo svolgimento di attività del proprio ufficio e al perseguimento delle finalità istituzionali del Comune di Ancona.**

Con tale preposizione la SV è autorizzata ad accedere ai dati personali limitatamente all'esecuzione dei compiti e all'esercizio delle mansioni del servizio di appartenenza, in base al profilo professionale e alla categoria di inquadramento.

Le operazioni di trattamento, che gli addetti al servizio sono autorizzati a svolgere, sono individuate e descritte in modo puntuale ed analitico nell'allegato al Documento Programmatico sulla Sicurezza, recante l'elenco dei trattamenti (ripartiti per singolo servizio e redatto ed aggiornato a cura del sottoscritto responsabile, per quanto di propria competenza).

Il documento è reso disponibile sull'Intranet del Comune alla voce "Privacy" oppure se ne può richiedere una copia al responsabile del servizio di appartenenza.

La SV ha l'obbligo, pertanto, di prendere visione dei trattamenti che possono essere svolti in seno al servizio di appartenenza, per i quali potrà ricevere, da parte del sottoscritto responsabile, ulteriori istruzioni o una ulteriore assegnazione di compiti maggiormente dettagliata.

La presente lettera di incarico è corredata da due allegati:

1) istruzioni e regole di comportamento alle quali ciascun incaricato deve attenersi;

2) linee guida, descrittive dei principi e delle regole base contenute nel Codice in materia di protezione dei dati personali.

Si informa che:

a) **titolare del trattamento** è il Comune di Ancona, come ente nel suo complesso, rappresentato dal Sindaco pro-tempore, secondo quanto previsto dall'art. 28 del codice della privacy.
b) responsabili del trattamento sono stati nominati, con apposito decreto del Sindaco, i dirigenti pro-tempore di ciascun servizio del Comune di Ancona, secondo quanto previsto nell'organigramma e nel regolamento dell'ordinamento dei servizi e degli uffici, ciascuno per quanto di propria competenza, con assegnazione dei compiti indicati nell'art. 6 del Documento Programmatico della Sicurezza (Aggiornamento 2008).

Si ricorda che la presente lettera deve essere sottoscritta solamente per ricevuta e costituisce un atto di documentata preposizione allo svolgimento di trattamenti, necessario per consentire a ciascun dipendente o collaboratore del Comune di svolgere le operazioni di trattamento, che siano strumentali all'esercizio delle mansioni e dei compiti istituzionali.

Responsabile del trattamento
(il Dirigente della Struttura)

Incaricato del trattamento
(per ricevuta e presa visione)

Allegato 1)

Il presente documento, allegato alla lettera di incarico, descrive le regole e le istruzioni che ciascun operatore, autorizzato ad accedere ai dati personali e al trattamento dei dati personali del Comune di Ancona, deve osservare.

Si ricorda che l'accesso ai dati è autorizzato nei limiti in cui le operazioni e le informazioni siano necessarie per il corretto svolgimento delle attività affidate, nonché per l'esecuzione dei compiti istituzionali del servizio dell'area o servizio di appartenenza.

a) Regole di comportamento e istruzioni per lo svolgimento delle operazioni di trattamento:

- **obbligo del segreto**: la regola fondamentale per garantire la tutela della riservatezza e della vita privata di persone fisiche e giuridiche è il segreto. Pertanto, ciascun dato o informazione, oggetto di conoscenza o di acquisizione, anche indiretta (come ad esempio nei casi di colloqui, visione di documenti, movimentazione di fascicoli, consegna a mano di corrispondenza,…), non deve essere utilizzato, se non esclusivamente per le finalità istituzionali e per lo svolgimento di mansioni e compiti relativi al servizio di appartenenza ovvero necessari per l'esecuzione degli obblighi e adempimenti oggetto di contratto di prestazione di servizio;

- **raccolta**: prima di procedere alla raccolta dei dati personali, deve essere fornita **l'informativa all'interessato** o alla persona presso cui si raccolgono i dati, ai sensi dell'art. 13 del codice privacy. L'ente ha predisposto la modulistica da utilizzare a tal proposito, disponibile anche in formato elettronico all'indirizzo - **{** HYPERLINK "http://www.comune.ancona.it" **}**) e sul link: Privacy della Intranet.

- occorre **procedere alla raccolta dei dati con la massima cura,** verificandone l'esattezza, nonché la pertinenza, la completezza e la non eccedenza rispetto alle finalità del trattamento, secondo quanto previsto dalla legge o dai regolamenti e le istruzioni del responsabile di servizio;

- **non lasciare dischetti, fogli, cartelle o altri supporti di memorizzazione** a disposizione di estranei;

- **conservazione**: i documenti o gli atti, che contengono dati sensibili o giudiziari o comunque riservati, devono essere custoditi e conservati in archivi ad accesso controllato. A tal proposito, ciascun responsabile del trattamento deve prevedere misure, da far rispettare ai propri incaricati, idonee a garantire che armadi, schedari e contenitori siano muniti di serratura ovvero che siano protetti contro accessi non controllati, adottando soluzioni (organizzative e procedurali), che consentano ai soli soggetti incaricati del trattamento di conoscere le informazioni detenute;

- i dati possono essere utilizzati solo dai soggetti espressamente incaricati. L'utilizzo dei dati deve avvenire per scopi determinati, espressi e legittimi e si deve evitare un utilizzo diverso rispetto alle finalità istituzionali dell'ente o non compatibile con le stesse;

- **comunicazione**: con tale espressione si intende "il 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". Ciò che caratterizza l'operazione di comunicazione è il fatto che un soggetto determinato (in posizione di terzietà rispetto al Comune e all'interessato) possa in qualunque forma conoscere dati personali riferiti all'interessato medesimo;

- **comunicazione di dati sensibili:** i dati sensibili possono essere comunicati a soggetti determinati solo ove sia espressamente previsto da una legge, che autorizzi tale operazione, ovvero dal regolamento sui dati sensibili e giudiziari. Si ricorda che il Consiglio Comunale, in conformità al parere del Garante per la protezione dei dati personali, ha adottato un apposito regolamento, disponibile e visionabile in intranet;

- **comunicazione di dati cd**. **comuni:** la comunicazione di dati comuni (ossia diversi da quelli sensibili) può avvenire solo se espressamente prevista da una legge o da un regolamento (cfr. art. 19, comma 3 del codice della privacy). Solamente nei confronti di altri soggetti pubblici, in via residuale, la comunicazione dei cd. dati comuni può avvenire ove sia necessaria per l'esercizio di una finalità istituzionale dell'ente destinatario della comunicazione stessa. In tal caso, tuttavia, occorrerà segnalare la circostanza al proprio responsabile, affinché proceda alla comunicazione preventiva al Garante per la protezione dei dati personali;

- **diffusione**: con tale espressione si intende "il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione". La pubblicazione di qualsiasi atto (all'albo pretorio o in una bacheca, ovvero in Internet), che contenga dati personali, costituisce, ai sensi del codice della privacy, una forma di diffusione di informazioni personali. Si ricorda che **l'art. 22, comma 8 del codice privacy vieta espressamente la diffusione di dati personali idonei a rivelare lo stato di salute.** Sarà cura quindi dei soggetti che redigono gli atti (deliberazioni e determinazioni) da pubblicare far sì che si rispetti il divieto considerato. Sul punto il Comune ha l'obbligo di adottare uno specifico regolamento, che è reso conoscibile a ciascun incaricato, con la massima pubblicità. A titolo meramente esemplificativo, si suggerisce la necessità di predisporre la copia degli atti da pubblicare, in una forma per cui il testo sia corredato da allegati (nei quali inserire i dati sanitari, che non potranno essere oggetto di pubblicazione, ma rimanere agli atti, a disposizione per eventuali istanze di accesso); in alternativa, nell'atto da pubblicare si potranno inserire *omissis* relativi ai dati da proteggere (stati, fatti e qualità idonei a rivelare lo stato di salute o un bisogno di natura sociale) ovvero sostituire all'identità del soggetto le sole iniziali. Della forma prescelta si dovrà dare evidenza nel testo della deliberazione e della determinazione, per giustificare che la copia destinata alla pubblicazione non sarà conforme all'originale, al fine di rispettare il divieto di diffondere i dati idonei a rivelare lo stato di salute.

- **diritto di accesso ai dati personali (art. 7 e segg. D. Lgs. 196/03**):occorre dare prontamente soddisfazione alle richieste che i soggetti interessati possono rivolgere, conformemente a quanto prescritto dall'art. 7 (Diritto di accesso ai dati personali ed altri diritti) e dall'art. 10 (Riscontro all'interessato) del D. Lgs. 196/2003, segnalando al Dirigente di Area o di Servizio il contenuto delle istanze. Quest'ultimo ha facoltà di individuare un preposto al riscontro delle istanze da parte degli interessati.

Qualora un incaricato del trattamento, nello svolgimento della propria attività lavorativa, si trovasse nella situazione di dover procedere ad una comunicazione o alla diffusione di dati, in mancanza di una espressa disposizione di legge o di regolamento (o vi siano dubbi al riguardo, sulla copertura normativa), è invitato a rivolgersi al Dirigente di area o di servizio per ricevere le istruzioni del caso.

b) Istruzioni per il corretto utilizzo degli strumenti elettronici:

- **computer:** tutte le volte che si abbandona la propria postazione di lavoro, si devono adottare accorgimenti per garantire che i dati trattati e memorizzati con elaboratori informatici non siano accessibili a soggetti non autorizzati. A tal proposito, si ricorda di non comunicare a terzi la propria password di accesso e di adottare misure di protezione: queste possono consistere in

uno *screen saver* con password; ovvero nella sospensione della sessione di lavoro, attraverso la disconnessione dell'applicazione in uso;

- **email e uso dell'Internet:** la posta elettronica deve essere utilizzata per scopi istituzionali di ufficio. Si ricorda che qualunque comunicazione ricevuta o spedita utilizzando l'indirizzo di posta del Comune non ha natura di corrispondenza personale. Le modalità operative di utilizzo degli strumenti di comunicazione elettronica e le tipologie di controllo e di accertamento sono riportate nel **Regolamento relativo all'accesso e all'uso della rete informatica e telematica, che ciascun operatore ha l'obbligo di visionare e conoscere mediante accesso diretto alla Intranet del Comune**.

  In calce ai messaggi di posta elettronica, è opportuno inserire la seguente formula:

  AVVISO DI PROTEZIONE

  La presente comunicazione può avere natura riservata, per cui i destinatari devono evitare di inoltrare a terzi il messaggio ricevuto, se non previa autorizzazione del mittente o quando vi sia una necessità personale o una giusta causa.
  Si informa che, utilizzando la posta elettronica di lavoro, eventuali risposte al presente messaggio potranno essere conosciute nell'organizzazione di appartenenza da soggetti incaricati per iscritto.
  Qualora sia stato inoltrato per errore un messaggio ad un soggetto non legittimato, quest'ultimo è pregato cortesemente di darne avviso al mittente e di procedere alla immediata cancellazione del testo dalla propria casella di posta elettronica.
  Si ricorda che la memorizzazione o la conservazione di informazioni ricevute erroneamente o senza averne titolo costituisce un comportamento sanzionabile dal codice della privacy (d. lgs. 196/2003).

- **protezione dei dati particolari:** occorre fare particolare attenzione alla spedizione, a mezzo di posta elettronica, di file o di messaggi contenenti dati sensibili. In tal caso, occorrerà proteggere il contenuto del file dall'accesso e dalla visione di soggetti non autorizzati o legittimati al trattamento, diversi dai destinatari delle comunicazioni elettroniche considerate. A titolo meramente esemplificativo, si consiglia (a seconda dei casi, da valutarsi a cura del responsabile del trattamento) il ricorso all'uso di tecniche di criptazione o di cifratura dei messaggi, ovvero all'utilizzo di codici identificativi dell'identità dell'interessato associati ai dati sensibili e giudiziari, in modo da rendere inintelligibili i dati in caso di intercettazione delle comunicazioni;

- **file di log:** per ragioni di sicurezza, si può avere la necessità di installare dispositivi automatizzati di registrazione delle operazioni svolte con elaboratori elettronici (cd. file di log) ovvero delle connessioni a Internet o dell'uso della posta elettronica;

- **fax:** questo strumento appare utile a garantire efficienza, economicità e velocità di comunicazione; tuttavia, presenta rischi specifici riguardo all'identità (a volte sconosciuta) di colui che materialmente riceve il documento trasmesso.

  Istruzioni per l'utilizzo del fax:

  - digitare correttamente il numero di telefono, cui inviare la comunicazione;
  - controllare l'esattezza del numero digitato prima di inviare il documento;
  - verificare che non vi siano inceppamenti della carta ovvero che non vengano presi più fogli contemporaneamente;
  - attendere la stampa del rapporto di trasmissione, verificando la corrispondenza tra il numero di pagine da inviare e quelle effettivamente inviate;
  - qualora vengano trasmessi dati idonei a rivelare lo stato di salute, può essere opportuno anticipare l'invio del fax chiamando il destinatario della comunicazione al fine di assicurarsi che il ricevimento avverrà nelle mani del medesimo, evitando che soggetti estranei o non autorizzati, possano conoscere il contenuto della documentazione inviata;
  - in alcuni casi, può essere opportuno richiedere una telefonata che confermi da parte del destinatario la circostanza della corretta ricezione e leggibilità del contenuto del fax;

  Formula consigliata da inserire in calce alla copertina di accompagnamento delle comunicazioni a mezzo fax:
  "Qualora il destinatario del presente fax non sia la persona indicata nella presente copertina, è pregato di dare immediata comunicazione al mittente, a mezzo telefono o per

fax. Successivamente, si prega di distruggere la documentazione erroneamente ricevuta, con l'avvertimento che in caso di non ottemperanza a questo invito si potrà essere responsabili della mancanza di protezione o dell'uso non autorizzato delle informazioni erroneamente acquisite".

- **telefono:** non fornire dati e informazioni di carattere sanitario o di natura comunque riservata per telefono, qualora non si conosca o non si abbia una verosimiglianza dell'identità o della legittimazione a conoscere del soggetto chiamante. In alcuni casi, può essere opportuno richiedere l'identità del chiamante e la propria qualità, provvedendo a richiamare, al fine di avere la certezza sull'identità del richiedente. Queste precauzioni non valgono nel caso di dati personali soggetti a pubblicazione (si pensi, a titolo meramente esemplificativo, ai dati di graduatorie di concorso, ovvero di selezioni pubbliche – appalti, conferimenti di incarichi), per cui il soggetto chiamante può conoscere i propri dati e quelli riferiti a soggetti terzi senza alcuna limitazione;

- **scanner**: i soggetti che provvedano all'acquisizione in formato digitale della documentazione cartacea (utilizzando ad esempio uno scanner) devono verificare che l'operazione avvenga correttamente e che il contenuto del documento oggetto di scansione sia correttamente leggibile; qualora vi siano errori di acquisizione ovvero si verifichino anomalie di processo, occorrerà procedere alla ripetizione delle operazioni;

- i **supporti informatici di memorizzazione**, già utilizzati per il trattamento dei dati sensibili e giudiziari, **devono essere riutilizzati solo se le informazioni precedentemente contenute non sono più in alcun modo recuperabili**, dovendo **altrimenti** essere **distrutti**. Tali dispositivi, qualora contengano dati personali, devono essere conservati in contenitori muniti di serratura;

- **spedizione di documenti contenenti dati personali a mezzo posta:** la documentazione contenente dati sensibili o giudiziari deve essere trasferita, anche all'interno dell'ente, in busta chiusa, in modo da proteggere la riservatezza del documento e dei dati contenuti. I lembi della busta devono essere sigillati e firmati per garantire l'integrità del contenuto;

- **uso di software:** è vietato installare e usare qualunque software, anche se scaricato da internet, senza la previa autorizzazione da parte del responsabile del trattamento. Si ricorda che l'uso di software contraffatto, ovvero senza licenza d'uso, costituisce un illecito, sia di natura penale, sia civile, secondo quanto previsto dalla legge sul diritto d'autore (legge 633/1941), così come integrata dal d. lgs. 518/1992 e successive modificazioni e integrazioni;

c) Regole per operatori di front-office e per la gestione di documenti cartacei:

- rispetto della **distanza di sicurezza:** per quanto riguarda gli operatori di sportello (cd. front-office ad esempio anagrafe e stato civile) deve essere prestata particolare attenzione al rispetto dello spazio di cortesia e se del caso invitare gli utenti a sostarsi dietro la linea tracciata sul pavimento ovvero dietro le barriere delimitanti lo spazio di riservatezza;

- **identificazione dell'interessato**: nei rapporti di sportello con l'utenza, può essere necessario identificare il soggetto interessato, al fine di verificare l'identità della persona e garantire l'esattezza del dato da raccogliere. A tal proposito è legittimo richiedere e ottenere un documento di identità o di riconoscimento;

- **controllo dell'esattezza del dato:** fare attenzione alla digitazione ed all'inserimento dei dati identificativi e personali degli interessati, evitando errori di battitura, che potrebbero creare problemi nella gestione dell'anagrafica e nel proseguo del processo;

- **tenuta di cartelle e di fascicoli:** cartelle e fascicoli tenuti sulla propria scrivania, qualora si ricevano nella propria stanza utenti e cittadini, devono essere trattati in modo da garantire la riservatezza degli interessati. Si consiglia di rivoltare sotto sopra le cartelle ovvero di

inserire (a seconda delle necessità operative e organizzative) sul frontespizio dati e informazioni per cui non sia resa conoscibile a terzi estranei l'identità dei soggetti interessati;

- **distruzione delle copie cartacee**: evitare di gettare la documentazione nel cestino della carta straccia senza aver previamente provveduto a rendere inintelligibile il contenuto: si potranno utilizzare apparati distruggi documenti o altri sistemi (ad esempio provvedere a stracciare i documenti; separare il dato identificativo dal resto delle informazioni mediante separazione fisica dei fogli,…);

d) Misure di protezione dei dati e degli strumenti elettronici

a) parola chiave:

- la parola chiave, assegnata a ciascun incaricato, deve essere composta da un minimo di otto caratteri o comunque dal numero massimo di caratteri consentito dal sistema;
- la parola chiave deve essere autonomamente cambiata dall'incaricato ogni sei mesi (nel caso di trattamento di dati personali comuni) ovvero con cadenza trimestrale (per il trattamento di dati sensibili o giudiziari). Per omogeneità di comportamenti, si deve procedere al **cambio della propria parola chiave al massimo ogni tre mesi**;
- la password non deve contenere riferimenti agevolmente riconducibile all'incaricato e dovrebbe essere generata preferibilmente senza un significato compiuto;
- l'incaricato, nello scegliere la propria password, deve preferibilmente utilizzare anche caratteri speciali e lettere maiuscole e minuscole;
- la parola chiave deve essere custodita con la massima attenzione e segretezza e non deve essere comunicata a terzi, per alcun motivo o ragione;
- l'incaricato è responsabile di ogni utilizzo indebito o non consentito della parola chiave, di cui sia titolare;
- ove vi sia la necessità di garantire la disponibilità dei dati e dei documenti a persone terze, deve essere richiesta l'abilitazione al responsabile dei sistemi informativi e ogni incaricato deve poter accedere con la propria credenziale di autenticazione;

b) **back-up:** salvo che non sia previsto un sistema di salvataggio di dati personali automatico ovvero centralizzato, occorre procedere con cadenza almeno settimanale alla effettuazione di copie di sicurezza dei dati personali oggetto di trattamento, utilizzando gli apparati che siano messi a disposizione dell'incaricato e consegnare i supporti contenenti le copie di salvataggio al soggetto nominato e incaricato della conservazione, ovvero riporre le copie in un contenitore al quale possano accedere solamente soggetti autorizzati;

c) **antivirus:** a meno che non siano adottati strumenti automatici di aggiornamento dei sistemi di protezione da programmi antivirus, gli incaricati del trattamento devono procedere all'effettuazione delle operazioni di aggiornamento dei programmi ivi considerati, almeno con cadenza settimanale o quando venga segnalata dal sistema tale esigenza, secondo le istruzioni visualizzate sullo schermo; una volta scaricato l'aggiornamento occorre procedere alla scansione dell'intero sistema per verificare la presenza sull'elaboratore in dotazione di virus;

d) **conservazione supporti rimovibili:** i supporti utilizzati per la memorizzazione di copie di file di documenti di lavoro non devono essere lasciati in luoghi accessibili. Si consiglia di riporre cd-rom, floppy disk, dispositivi di memorizzazione in cassetti muniti di serratura ovvero di custodire gli stessi in modo da garantire un accesso controllato.

Allegato 2)

Cosa sono i dati personali

La legge definisce dato personale “qualunque informazione relativa a persona fisica, persona giuridica, ente o associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale”.

Sono tre le tipologie di dati personali che possono essere trattati:

1) **sensibili**: sono 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”;
2) **giudiziari**: sono i dati 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”;
3) **dati comuni**: sono le informazioni riferite a persona fisica, persona giuridica, ente o associazione, identificati o identificabili, anche indirettamente differenti dai dati idonei a rivelare gli stati, fatti e le qualità per cui il legislatore definisce le informazioni di natura sensibile o giudiziaria. Questi dati, di conseguenza, si ricavano per esclusione e in via residuale.

In base a quanto previsto dagli articoli 18 e seguenti del D. Lgs. n. 196/2003, un ente pubblico può trattare dati personali comuni solo per lo svolgimento di funzioni istituzionali; i dati sensibili e giudiziali possono essere trattati soltanto se vi è una specifica autorizzazione, da parte di una norma di legge o di regolamento.

Cosa è il trattamento dei dati personali

La legge definisce trattamento dei dati personali “qualunque operazione o complesso di operazioni concernenti la raccolta, la registrazione, l’organizzazione, la conservazione,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 dei dati”.

E’ indifferente che le operazioni vengano svolte con o senza l’ausilio di mezzi elettronici, o comunque automatizzati, per cui anche i trattamenti effettuati su supporto cartaceo sono assoggettati alla normativa sulla tutela della privacy.

Le operazioni, che caratterizzano ciascun processo di trattamento, possono essere di tre tipi:

- il reperimento delle informazioni;

- il trattamento interno;

- l'uso delle informazioni nei rapporti con l'esterno.

1. Il reperimento delle informazioni

Tale fase, tecnicamente definita “raccolta di dati”, riguarda l’acquisizione delle informazioni, in qualunque modo essa avvenga: ad esempio, direttamente dalla persona interessata, presso terzi, o mediante consultazione di elenchi.

2. Il trattamento interno delle informazioni

Tale fase raggruppa le varie operazioni poste in essere da chi raccoglie informazioni per organizzarle e renderle agevolmente usufruibili.

Esse sono:

- la registrazione dei dati, cioè il loro inserimento in supporti, automatizzati o manuali, alfine di rendere i dati disponibili per i successivi trattamenti;

- la organizzazione dei dati in senso stretto, cioè il processo di trattamento che ne favorisca la fruibilità attraverso l'aggregazione o la disaggregazione, l'accorpamento, la catalogazione, eccetera;

- la elaborazione, cioè le operazioni che attribuiscono significatività ai dati in relazione allo scopo per il quale essi sono stati raccolti;

- la selezione, la estrazione ed il raffronto, che sono operazioni specifiche che rientrano nella ipotesi più generale della elaborazione;

- la modificazione dei dati registrati, in relazione a variazioni o a nuove acquisizioni di dati;

- la interconnessione, ovvero la messa in relazione di banche dati diverse e distinte tra loro al fine di compiere ulteriori processi di elaborazione, selezione, estrazione o raffronto;

- il blocco, ovvero la conservazione dei dati con sospensione temporanea dei trattamenti;

- la conservazione dei dati (alla quale la legge dedica particolari attenzioni sotto il profilo della sicurezza);

- la cancellazione o la distruzione dei dati, che sono operazioni il cui compimento fa sorgere l'obbligo di effettuare taluni specifici adempimenti.

3. L’uso delle informazioni nei rapporti con l’esterno

E’ la fase che comprende i trattamenti più delicati: essi vengono genericamente definiti come “utilizzo”, cioè la realizzazione dello scopo per cui si è provveduto alla raccolta ed ai trattamenti interni.

L’utilizzo può essere:

 diretto, instaurando cioè un rapporto con la persona sul conto della quale si sono raccolte le informazioni

 ovvero consistere nel mettere a disposizione di terzi le informazioni raccolte.

Le operazioni di utilizzo, cui la legge dedica le maggiori attenzioni, sono quelle che hanno ad oggetto la messa a disposizione di terzi dei dati personali raccolti e trattati dal Comune.

Esse sono:

 la comunicazione, cioè il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione.

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

In base a quanto previsto dagli articoli 18 e seguenti del D. Lgs. n. 196/2003, 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.

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.

Si ricorda che ogni incaricato del trattamento, nel trattare i dati personali, deve rispettare i seguenti principi:

1) principio di finalità (previsto dall'art. 11 lettera b) del codice privacy): il trattamento deve essere svolto per scopi determinati, espliciti e legittimi. Con riferimento ai soggetti pubblici, questo limite è ancor più pregnante, considerato che le pubbliche amministrazioni possono procedere al trattamento solamente se il trattamento è strumentale allo svolgimento di funzioni istituzionali (ai sensi dell'art. 18, comma 2 del codice della privacy), senza dover richiedere il consenso degli interessati al trattamento. Questa regola ha solamente due eccezioni, riguardanti gli organismi sanitari pubblici, ai sensi dell'art. 76 e 110 del codice privacy, i quali prevedono rispettivamente che i dati idonei a rivelare lo stato di salute possono essere trattati solo con il consenso dell'interessato per finalità di tutela della salute o dell'incolumità fisica dell'interessato o di ricerca scientifica in campo medico, biomedico o epidemiologico;

2) **principio di proporzionalità** (art. 11 lettera d) del codice privacy): i dati, oggetto di trattamento, devono essere pertinenti, non eccedenti e completi rispetto agli scopi istituzionali perseguiti. La pertinenza attiene al merito dell'attività di trattamento; la non eccedenza alla quantità dei dati che possono essere raccolti e trattati in riferimento allo scopo perseguito; infine, la completezza attiene alla tutela dell'identità personale dell'interessato, che ha interesse a che il suo profilo e le informazioni detenute non sia parziali. Ove il trattamento riguardi dati sensibili o giudiziari, occorre verificare caso per caso che i dati (di questa specie) siano indispensabili rispetto alla finalità perseguita;

3) **principio di necessità** (art. 3 del codice): che richiede che “i sistemi informativi e i programmi informatici siano configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità”. A questo principio generale, si aggiunge l’obbligo della cd. disgiunzione logica dei dati personali, che richiede di adottare una serie di misure di protezione in modo da consentire l’identificazione dell’interessato sono in caso di necessità, nelle ipotesi di trattamento di dati sensibili o giudiziari, con elenchi, registri e banche dati detenute con strumenti elettronici (art. 22, comma 6 del codice);

4) **principio di sicurezza** (articoli 31 e seguenti del codice privacy): i dati oggetto di trattamento devono essere protetti attraverso l’adozione di misure di sicurezza. Queste sono adottate a seguito dell’analisi e della valutazione dei rischi, che è svolta dall’Area Sistemi Informativi, per quanto riguarda i trattamenti svolti con strumenti elettronici, che richiedono un aggiornamento continuo con cadenza almeno annuale. Le misure di sicurezza sono, quindi, individuate e riportate nel documento programmatico sulla sicurezza (DPS). Gli incaricati del trattamento ricevono apposite istruzioni da parte dei responsabili del trattamento, con conseguente obbligo di rispetto delle misure di sicurezza e conseguenti possibili responsabilità, anche di natura penale, in caso di mancato rispetto delle istruzioni ricevute o delle misure previste.