COMUNE DI GENOVA

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA
Anno 2011

CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI
D. L.VO 196/2003

1. Principi generali

Il presente Documento Programmatico sulla Sicurezza (D.P.S.) costituisce una misura minima di sicurezza inerente il trattamento con strumenti elettronici dei dati personali sensibili e giudiziari. Il D.P.S. contiene informazioni e prescrizioni in base a quanto previsto dal D. L.vo 196/2003 e suoi allegati. Le prescrizioni, estese ai trattamenti di tutti i dati personali effettuati con qualsiasi strumento, costituiscono un punto di riferimento per il trattamento di tutte le informazioni da parte del Comune di Genova.

Attraverso le prescrizioni contenute nel D.P.S. l'Ente persegue i seguenti obiettivi:
1.1 ottemperanza agli adempimenti stabiliti da norme giuridiche o da provvedimenti emanati dalle Autorità competenti;
1.2 diffusione della cultura della protezione delle risorse produttive;
1.3 evidenziazione dell'importanza strategica e del valore delle informazioni;
1.4 razionalizzazione ed ottimizzazione dell'organizzazione, delle funzioni, dei processi e delle attività;
1.5 uniformità dei principi di trattamento delle informazioni e dei dati;
1.6 adozione di standard procedurali e tecnici;
1.7 incentivazione al decentramento operativo;
1.8 efficacia dei processi e delle attività trasversali alla struttura;
1.9 valorizzazione e responsabilizzazione del personale;
1.10 formazione permanente del personale.

In base alle caratteristiche della struttura e dell'organizzazione dell'Ente, descritte nel Regolamento sull'ordinamento degli uffici e dei servizi, alle attività istituzionali previste ed ai compiti e responsabilità dei Dirigenti, il D.P.S. indica i criteri programmatici cui i Dirigenti, così come individuati al punto 3.1, in qualità di Responsabili dei trattamenti, devono attenersi per garantire la protezione dei dati. L'impostazione adottata riflette l'articolazione dell'Ente, organizzato in unità operative connotate da specificità tali da non consentire la definizione di modalità di trattamento standardizzate o automaticamente applicabili a tutta la struttura comunale.

L'attuazione delle prescrizioni contenute nel D.P.S. è basata sul principio della documentazione delle procedure, in conformità alle norme vigenti. Tutte le attività volte a garantire la sicurezza dei dati personali devono essere effettuate secondo procedure conformi alle linee guida dell'Ente.

2. Definizioni

Il presente D.P.S. recepisce le definizioni contenute nell'articolo 4 del D. L.vo 196/2003, introducendone di nuove e apportando altresì alcune semplificazioni.

Ai fini della corretta interpretazione del documento, si intende per:
Dato ultrasensibile: dato personale sensibile idoneo a rivelare lo stato di salute o la vita sessuale dell'interessato.
Minaccia: un potenziale evento dannoso conosciuto, in grado di compromettere la sicurezza dei dati.
Obiettivo di Intervento (O.I.): il contesto fisico o logico ove avviene il trattamento dei dati, ovvero l'oggetto sul quale ricadono le minacce e devono pertanto essere applicate le misure di sicurezza.
Rischio: la probabilità di accadimento di una minaccia, ponderata rispetto al danno che può provocare.
Sicurezza: l'autenticità, l'integrità, la disponibilità e la riservatezza dei dati.
Sistema informatico: il sistema di gestione automatizzata delle informazioni nell'ambito di un'organizzazione.
Sistema informativo: il sistema di gestione di tutte le informazioni nell'ambito di un'organizzazione.
Supporto di trattamento: l'elemento materiale su cui vengono memorizzati, elaborati e trasmessi i dati.
Vulnerabilità: l'attitudine intrinseca di una risorsa a subire gli effetti della realizzazione di una minaccia.

3. Informazioni sulla distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati

3.1 Figure preposte al trattamento e altre figure

Titolare del trattamento dei dati personali è la Civica Amministrazione, nella persona del Sindaco pro tempore.

I Responsabili interni del trattamento dei dati personali sono i Dirigenti, ciascuno per quanto concerne l'ambito di competenza.

Gli Incaricati del trattamento dei dati personali sono le persone fisiche designate dai Responsabili ad effettuare trattamenti di dati personali.

I Referenti sono le persone fisiche designate dai Responsabili per svolgere, in materia di trattamento dei dati personali, le funzioni di cui al punto 3.4.

Il "Gruppo di lavoro per l'applicazione della normativa sulla protezione dei dati personali" è istituito con provvedimento del Sindaco per svolgere le funzioni di cui al punto 3.5.

Gli Amministratori di sistema sono le persone fisiche individuate nell'allegato "A" al presente Documento, dal Titolare su proposta dei Responsabili, per svolgere le funzioni di cui al punto 3.6.

3.2 Compiti del Titolare

Il Titolare:

3.2.1 nomina i Responsabili, interni ed esterni, del trattamento;

3.2.2 informa tempestivamente i Responsabili, tramite il "Gruppo di lavoro per l'applicazione della normativa sulla protezione dei dati personali", circa gli aggiornamenti della normativa in materia di trattamento di dati personali, nonché in merito alle regole che definiscono i compiti degli stessi;

3.2.3 assume, su proposta dei Responsabili, le decisioni in ordine alle finalità e alle modalità del trattamento, anche con riguardo agli strumenti utilizzati o utilizzabili e sotto il profilo della sicurezza;

3.2.4 acquisisce le relazioni annuali dei Responsabili circa lo stato di attuazione della normativa in materia di trattamento dei dati personali;

3.2.5 effettua controlli sull'operato dei Responsabili interni, anche verificando la conformità al D.P.S. delle procedure adottate;

3.2.6 coordina l'applicazione delle misure di sicurezza;

3.2.7 aggiorna annualmente il D.P.S. ;

3.2.8 individua, su proposta dei Responsabili, gli Amministratori di sistema, riportandone gli estremi identificativi e le funzioni ad essi attribuite nell'allegato "A" al D.P.S.;

3.2.9 verifica la rispondenza dell'operato degli Amministratori di sistema alle misure organizzative, tecniche e di sicurezza previste dalla legge per i trattamenti dei dati personali.

3.3 Compiti dei Responsabili

Il Responsabile:

3.3.1 individua le norme di legge o di regolamento, i fini istituzionali o le rilevanti finalità di interesse pubblico in base ai quali deve o può essere effettuato un trattamento di dati personali;

3.3.2 formula proposte al Titolare circa le decisioni da assumere in ordine alle finalità e alle modalità del trattamento, anche con riguardo agli strumenti utilizzati o utilizzabili e sotto il profilo della sicurezza;

3.3.3 effettua le comunicazioni e provvede agli altri adempimenti previsti dalla normativa vigente nei confronti del "Garante per la Protezione dei Dati Personali" o di altri organismi ispettivi;

3.3.4 istituisce e gestisce le banche di dati di competenza, redigendone l'elenco;

3.3.5 classifica i dati in base alla loro natura e tipologia, nel momento in cui vengono acquisiti o generati, ovvero ne viene modificata la natura o la struttura in seguito a trattamento;

3.3.6 individua i trattamenti di competenza, redigendone l'elenco;

3.3.7 stabilisce le procedure e le modalità di effettuazione dei trattamenti, individuando gli strumenti utilizzabili;

3.3.8 predispone la scheda per l'informativa ed attua tutti gli accorgimenti per garantire l'esercizio dei diritti dell'interessato;

3.3.9 individua i luoghi fisici in cui sono allocate le banche di dati ed in cui vengono effettuati i trattamenti;

3.3.10 individua gli Obiettivi di Intervento (O.I.);

3.3.11 effettua l'Analisi dei Rischi (A.R.);

3.3.12 ottempera alle disposizioni del D.P.S.;

3.3.13 adotta le misure minime di sicurezza previste dalla normativa vigente e tutti gli altri accorgimenti necessari per prevenire la distruzione, la perdita o l'alterazione dei dati, l'accesso ed i

trattamenti non autorizzati o non conformi alle finalità del trattamento, nonché per assicurarne la disponibilità ai fini del trattamento e per garantire l'esercizio dei diritti dell'interessato;
3.3.14 definisce i profili degli Incaricati in base alla necessità di accedere ai dati e di effettuare i trattamenti;
3.3.15 nomina per iscritto gli Incaricati, in base alle competenze ed ai trattamenti effettuati dagli uffici;
3.3.16 nomina almeno un Referente per la protezione dei dati personali;
3.3.17 definisce i programmi di formazione degli Incaricati, secondo i principi espressi nel D.P.S.;
3.3.18 effettua controlli sui trattamenti di competenza, compresi quelli esternalizzati;
3.3.19 comunica tempestivamente al Titolare situazioni di criticità o di rischio a carico dei dati personali e dei trattamenti di competenza;
3.3.20 elabora, entro il 28 Febbraio di ogni anno, una relazione con la quale riferisce al Titolare in merito alla gestione dei dati personali effettuata dalla struttura di competenza nel corso dell'anno precedente formulando, se del caso, osservazioni e proposte;
3.3.21 predispone i provvedimenti del Titolare in materia di trattamento dei dati, ivi compresa la nomina di Responsabili di trattamento esterni all'Ente;
3.3.22 individua e nomina per iscritto i soggetti esterni Incaricati di trattamento e definisce modalità e standard, sia tecnici che organizzativi, per l'effettuazione dei trattamenti medesimi, accertando che le prescrizioni siano formalmente accettate e sostanzialmente applicate dai soggetti esterni;
3.3.23 stabilisce i casi in cui i dati devono essere comunicati, nonché le relative modalità di comunicazione;
3.3.24 concorda formalmente, in caso di trattamento congiunto con strutture interne facenti capo ad altri Responsabili, procedure, modalità di trattamento, strumenti utilizzabili, operazioni eseguibili e misure di sicurezza, sulla base delle competenze attribuite dall'Amministrazione alle singole strutture;
3.3.25 attua quanto non sia espressamente previsto dal presente D.P.S., al fine di garantire la puntuale applicazione della normativa vigente in materia di trattamento e protezione dei dati personali;
3.3.26 propone al Titolare i nominativi degli Amministratori di sistema per l'aggiornamento periodico dell'elenco di cui all'allegato "A" al D.P.S.;
3.3.27 vigila sull'operato degli Amministratori di sistema, riferendone al Titolare;
3.3.28 adotta sistemi di controllo che consentano la registrazione degli accessi effettuati dagli Amministratori di sistema ai sistemi di elaborazione e agli archivi elettronici.

3.4 Compiti dei Referenti

Il Referente:
3.4.1 svolge attività di consulenza presso la struttura di appartenenza;
3.4.2 svolge, su delega del Responsabile, attività di coordinamento all'interno della struttura di competenza;
3.4.3 effettua interventi di formazione interna;
3.4.4 mantiene rapporti con il "Gruppo di lavoro per l'applicazione della normativa sulla protezione dei dati personali" per conto del Responsabile di riferimento.

3.5 Compiti del "Gruppo di lavoro per l'applicazione della normativa sulla protezione dei dati personali"

Il "Gruppo di lavoro per l'applicazione della normativa sulla protezione dei dati personali":
3.5.1 informa tempestivamente i Responsabili, anche attraverso i Referenti, circa gli aggiornamenti della normativa in materia di trattamento di dati personali, nonché in merito agli adempimenti di loro competenza;
3.5.2 collabora con il Titolare e i Responsabili alla predisposizione di atti dell'Ente;
3.5.3 effettua attività di consulenza all'interno dell'Ente;
3.5.4 mantiene rapporti con i Referenti e, tramite questi, con i Responsabili;
3.5.5 contribuisce a pianificare gli interventi di formazione nei casi previsti al punto 8.

3.6 Compiti degli Amministratori di sistema

All'Amministratore di sistema compete:
3.6.1 la gestione e la manutenzione di un impianto di elaborazione o di sue componenti e delle reti ad esso connesse;
3.6.2 la vigilanza sulla corretta utilizzazione del sistema informatico, attenendosi alle misure organizzative, tecniche e di sicurezza previste dalla legge e dall'Ente.

4. Informazioni sull'elenco dei trattamenti dei dati personali

4.1 Elenco delle banche di dati

Il Responsabile redige l'elenco delle banche di dati personali di competenza e ne cura la conservazione e l'aggiornamento.

Ad ogni banca di dati viene attribuito un codice che indica:
- la sua identità;
- l'eventuale soggetto esterno, diverso dall'interessato, da cui si acquisisce;
- il soggetto interno proprietario.

L'elenco, per ogni banca di dati, deve indicare:
- il codice di identità;
- l'ubicazione;
- i riferimenti documentali circa il contenuto della banca di dati;
- l'interconnessione con altre banche di dati.

4.2 Elenco dei trattamenti

Il Responsabile redige l'elenco dei trattamenti di dati personali di sua competenza e ne cura la conservazione e l'aggiornamento.
Ad ogni trattamento viene attribuito un codice che indica la sua identità.
L'elenco, per ogni trattamento e con riferimento ai compiti degli incaricati, deve indicare:
4.2.1 la sua identità;
4.2.2 l'identità della banca di dati in cui il dato trattato è registrato;
4.2.3 il tipo di dato trattato;
4.2.4 l'obiettivo del trattamento;
4.2.5 il presupposto giuridico del trattamento;

4.2.6 la descrizione sintetica del trattamento o le operazioni eseguibili;
4.2.7 i soggetti cui i dati devono essere eventualmente comunicati;
4.2.8 gli strumenti impiegati per il trattamento.

5. Informazioni sull'Analisi dei Rischi

L'Analisi dei Rischi (A.R.) ha natura dinamica e permanente. Viene predisposta al fine di mettere in relazione le risorse da proteggere, i rischi da cui sono interessate e le misure di sicurezza da adottare.

L'A.R. viene necessariamente effettuata negli stessi casi in cui è obbligatorio procedere con la formazione degli Incaricati (8).

L'A.R. prevede:
5.1 la classificazione del dato;
5.2 la valutazione del dato in base alla sua criticità (giuridica, economica, produttiva, immateriale);
5.3 la contestualizzazione del dato all'interno dell'architettura del sistema informativo, con principale riferimento alla localizzazione dei supporti di registrazione/memorizzazione, elaborazione e comunicazione/trasmissione;
5.4 la definizione degli Obiettivi di Intervento (O.I.) e della loro vulnerabilità;
5.5 l'individuazione delle minacce di cui sono oggetto gli O.I.;
5.6 l'analisi delle possibili modalità di accadimento delle minacce, in base alla loro natura (accidentale, colposa o dolosa) e origine (esterna o interna);
5.7 la considerazione e la misurazione delle conseguenze in caso di accadimento dell'evento dannoso;
5.8 la definizione, su base probabilistica, del livello di rischio;
5.9 la definizione di una scala di priorità in merito all'adozione di misure di sicurezza.

6. Informazioni sulle misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali rilevanti ai fini della loro custodia e accessibilità

Le misure di sicurezza vengono applicate al fine di garantire l'autenticità, l'integrità, la disponibilità e la riservatezza dei dati, con particolare riguardo alla prevenzione.

Per ogni O.I., individuato in base alla posizione fisica e logica delle banche dati e dei trattamenti nell'ambito del sistema informativo devono essere indicati, conseguentemente all'effettuazione dell'A.R.:
6.1 il codice della banca di dati;
6.2 il codice del trattamento;
6.3 la tipologia della misura adottata (tecnica, informatica, organizzativa, logistica, procedurale);
6.4 gli strumenti e le procedure adottate, nonché gli scopi perseguiti;
6.5 la stima del rischio residuo.

Ogni O.I. può comprendere più banche di dati e trattamenti. La protezione dell'O.I. deve essere ottimizzata al fine di perseguire congiuntamente la sicurezza delle persone e delle risorse materiali e immateriali dell'Ente a fronte di minacce di natura accidentale, colposa o dolosa, nonché di origine interna o esterna.

7. Informazioni su criteri e modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento

Il Responsabile garantisce la disponibilità dei dati adottando misure idonee per la loro duplicazione e per il ripristino delle banche di dati.

I criteri e le modalità per il ripristino della disponibilità dei dati, considerata l'Analisi dei Rischi, fanno riferimento a:
7.1 idoneità delle strutture (rispetto delle destinazioni d'uso, adeguamento, manutenzione, compartimentazione, gestione degli accessi e dei flussi, fruizione, gestione delle attività);
7.2 adozione di procedure per il controllo degli accessi alle risorse fisiche e logiche, per la duplicazione dei dati, per il ripristino delle banche di dati e, nei casi in cui è possibile, per la rigenerazione dei dati;
7.3 adozione di procedure per la duplicazione, informatizzata o mista, dei dati, nonché per la custodia separata delle banche di dati;
7.4 acquisizione, gestione e aggiornamento di tecnologie e di strumenti per il ripristino delle banche di dati;
7.5 controllo e manutenzione dei supporti di memoria e degli strumenti di trattamento.

8. Informazioni sulla previsione degli interventi formativi degli Incaricati

I Responsabili, di concerto con gli Uffici dell'Ente preposti alla formazione del personale, organizzano gli interventi formativi per gli Incaricati di trattamento ed i Referenti.

Gli interventi di formazione, limitatamente al personale interessato, sono obbligatori nei seguenti casi:

8.1 modificazione o integrazione della normativa di riferimento (*);
8.2 modificazione o integrazione delle norme dell'Ente (*);
8.3 variazione della struttura organizzativa dell'Ente;
8.4 ridefinizione delle competenze delle Direzioni e delle strutture subordinate;
8.5 adozione di nuove procedure per la sicurezza dei dati (*);
8.6 variazioni interne di una struttura;
8.7 assunzione di personale (*);
8.8 passaggio di categoria;
8.9 variazione di qualifica;
8.10 trasferimento ad altro Ufficio;
8.11 assegnazione ad altro incarico o mansione;
8.12 istituzione di nuovi trattamenti;
8.13 variazione o aggiornamento dei trattamenti;

8.14 istituzione di nuove procedure;
8.15 variazione o aggiornamento di procedure;
8.16 adozione di nuovi strumenti di trattamento;
8.17 adozione di nuovi strumenti per la sicurezza dei dati (*).

Gli interventi di formazione sono improntati al principio del più ampio decentramento, attraverso l'ausilio dei Referenti. Nei casi contrassegnati con l'asterisco (*), data la trasversalità delle materie, la formazione viene pianificata in collaborazione con il "Gruppo di lavoro per l'applicazione della normativa sulla protezione dei dati personali".
Il Responsabile predispone il piano di formazione e registra i corsi di formazione effettuati, dandone conto al Titolare nella relazione annuale. Il Responsabile svolge comunque opera di sensibilizzazione del personale, richiamando i principi cui si ispira la normativa in materia, i provvedimenti delle Autorità competenti, le regole dell'Ente e le prescrizioni contenute nel presente Documento Programmatico sulla Sicurezza.

9. Informazioni sui criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al Codice, all'esterno della struttura del Titolare

Nel caso di trattamenti affidati all'esterno della struttura del Titolare, il Responsabile inserisce nel Capitolato Speciale le clausole indicanti le direttive cui il soggetto esterno deve attenersi, specificando l'obbligo di conformità a quanto previsto nel presente D.P.S.. Le clausole devono prevedere l'obbligo di adottare autonomamente le misure minime di sicurezza previste dalla normativa vigente. Le clausole devono evidenziare la facoltà dell'Ente di effettuare controlli, a seguito dei quali possono essere applicate penali ovvero può essere risolto il contratto. In base all'A.R., il trattamento effettuato dal soggetto esterno deve garantire lo stesso livello di sicurezza previsto per lo stesso tipo di dati trattati all'interno.

10. Informazioni sui criteri da adottare per la cifratura o la separazione dei dati personali idonei a rivelare lo stato di salute e la vita sessuale (dati ultrasensibili) dagli altri dati personali dell'Interessato

Il Responsabile, con riguardo ai dati personali sensibili idonei a rivelare lo stato di salute e la vita sessuale dell'Interessato, individua le banche di dati ed i relativi trattamenti. Redige procedure per limitare i trattamenti ai soli casi indispensabili per lo svolgimento delle funzioni istituzionali e per gli adempimenti previsti dalla normativa vigente. Individua gli Incaricati del trattamento e ne descrive analiticamente i compiti, in base alle operazioni autorizzate. Disciplina l'accesso ai dati da parte degli Incaricati, sulla base del principio della "necessità di sapere" e del "minimo privilegio".

In caso di trattamento informatizzato, il Responsabile utilizza gli strumenti applicativi necessari per crittografare i dati sensibili idonei a rivelare lo stato di salute e la vita sessuale.

In caso di trattamento cartaceo, provvede a separare fisicamente e a custodire separatamente i dati personali da quelli ultrasensibili. All'Interessato viene abbinato un codice identificativo che

consenta di unificare le informazioni contenute in archivi separati. Nei documenti contenenti dati sensibili idonei a rivelare lo stato di salute e la vita sessuale l'Interessato è individuabile solamente mediante il codice sopra menzionato.