Documento programmatico sulla sicurezza

Oggetto

Il presente documento ha lo scopo di descrivere le misure di sicurezza organizzative, fisiche e logiche, da adottare per il trattamento dei dati personali, sensibili e giudiziari effettuato dalla Provincia di Reggio Emilia.

Il documento è redatto sulla base delle disposizioni di cui al Decreto Legislativo 30 giugno 2003, n.196, artt. da 33 a 36 (misure minime di sicurezza) nonché del disciplinare tecnico contenuto nell'allegato B del citato decreto. In particolare:

- l'art. 34, comma 1, lettera g) del D.Lgs. 196/2003 ora soppresso, prevedeva nel caso di trattamento di dati personali effettuato con strumenti elettronici, l'obbligo della "tenuta di un aggiornato documento programmatico sulla sicurezza": si ritiene di procedere ad aggiornare tale documento ai fini di attualizzare quanto approvato con Deliberazione di Giunta n. 96/2011, all'attuale assetto dell'Ente, modificato con L. 56/2014;
- il punto 19 dell'allegato B definisce le idonee informazioni necessarie per redigere il predetto documento, che di seguito viene più semplicemente definito DPS.

In particolare, sulla base delle regole previste dal disciplinare tecnico, il DPS è strutturato nelle seguenti sezioni:

1. l'elenco dei trattamenti di dati personali (*punto 19.1 del disciplinare*);
2. la distribuzione dei compiti e delle responsabilità, nell'ambito delle strutture preposte al trattamento dei dati (*punto 19.2 del disciplinare*);
3. l'analisi dei rischi che incombono sui dati (*punto 19.3 del disciplinare*);
4. le misure, già adottate e 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 (*punto 19.4 del disciplinare*);
5. i criteri e le modalità di ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento (*punto 19.5 del disciplinare*);
6. la previsione di interventi formativi degli incaricati del trattamento (*punto 19.6 del disciplinare*);
7. la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati affidati, in conformità al Codice della Privacy (D.Lgs.196/03) all'esterno della struttura del titolare (*punto 19.7 del disciplinare*);
8. dichiarazioni d'impegno.

La Presidente della Provincia con proprio decreto n. 67 del 14/12/2009 ha individuato l'elenco dei soggetti idonei a svolgere le mansioni di amministratore di sistema in ottemperanza al provvedimento del Garante "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" del 27 novembre 2008 e modificato con provvedimento del 25 giugno 2009.

Elenco dei trattamenti dei dati personali (19.1)

La Provincia di Reggio Emilia tratta i dati personali ai fini del conseguimento delle proprie finalità istituzionali nel rispetto dei vincoli e dei principi previsti dalla vigente disciplina, con particolare riguardo ai principi di necessità, pertinenza e non eccedenza.

In seguito alla L. 56/2014 e successive leggi regionali di riordino, si configura un diverso assetto organizzativo dell'Ente ed è quindi importante attualizzare alla nuova organizzazione l'elenco dei procedimenti rimasti in capo alla Provincia, descritti nell'Allegato A e l'elenco dei trattamenti effettuati presso i Servizi dell'Ente e delle relative

misure di sicurezza adottate, descritti nell'Allegato B.

Tali allegati hanno un valore di prima ricognizione, in quanto i procedimenti ed i relativi trattamenti saranno meglio analizzati nei prossimi mesi, dando piena applicazione al Regolamento UE 2016/679 in materia di protezione dei dati personali (GDPR) che istituisce l'obbligo del 'Registro delle attività di trattamento'.

Nei trattamenti elencati vengono utilizzati supporti sia cartacei che informatici.

Il trattamento dei dati sensibili e giudiziari è effettuato soltanto con le modalità consentite da norme di legge e dal “Regolamento per il trattamento dei dati sensibili e giudiziari” dell’Ente, adottato con deliberazione del consiglio provinciale n.4 del 12/01/2006.

A seguito della sopra citata L.56/2014 e successive leggi regionali di riordino, che hanno definito un diverso assetto organizzativo dell'Ente si è proceduto per i temi non più di competenza ad un complesso processo di trasferimento del personale, della documentazione e relative dotazioni tecnologiche al nuovo Ente di competenza. Tale processo non è attualmente completato e per alcuni settori il personale utilizza ancora parte della dotazione informatica, rete e banche dati in gestione all'UO Sistemi Informativi della Provincia di Reggio Emilia. In particolare per quanto riguarda le tematiche del lavoro e dei centri per l'impiego, una parte di archivio digitale, la posta elettronica e la rete utilizzata sono erogati dalla Provincia: su tali dati sono adottate tutte le misure di sicurezza adottate nel presente documento per garantire la tutela e la riservatezza dei dati ospitati.

Compiti e responsabilità (19.2)

Il Titolare dei dati, ai sensi della vigente disciplina, è la Provincia di Reggio Emilia che provvede ai compiti attribuiti a tale titolo dalla vigente disciplina in relazione alle competenze dei propri organi; in particolare e in via meramente esemplificativa, al Consiglio provinciale compete l'adozione delle norme regolamentari, mentre il Presidente provvede con propri atti alle nomine e all'adozione di norme di attuazione. La Provincia di Reggio Emilia è altresì responsabile dei trattamenti svolti per conto di altri titolari in forza di contratti, convenzioni, delega o attribuzioni di funzioni.

Anche in assenza di specifici provvedimenti, i dirigenti sono individuati quali responsabili del trattamento dei dati di pertinenza dell'area/servizio affidato.

All'atto dell'assunzione o di successive assegnazioni funzionali, i dipendenti sono contestualmente individuati come incaricati del trattamento dei dati in relazione ai compiti assegnati.

Analisi dei rischi che incombono sui dati (19.3)

L’analisi degli eventi potenzialmente dannosi per la sicurezza dei dati (minacce) e la stima dei rischi legati ad essi sono riportate nell'Allegato C.

Misure in essere e da adottare (19.4)

Le misure in essere per contrastare i rischi individuati nell’analisi del paragrafo precedente sono riportate nell'allegato C. Nello stesso allegato sono contenute informazioni riguardo la protezione delle aree e dei locali rilevanti ai fini della custodia e dell'accessibilità dei dati.

In ottemperanza al provvedimento del Garante “Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema”, sono stati adottati sistemi idonei alla registrazione degli accessi logici ai sistemi di elaborazione e agli archivi elettronici da parte degli

amministratori di sistema, secondo le specifiche minime previste dal provvedimento stesso.

E' stato revisionato il documento (Allegato F) contenente le procedure di intervento in caso di emergenze quali incendio, furto di strumentazione informatica, interruzione di corrente, surriscaldamento dei server, allagamento della sala macchine, interruzione della connettività.

E' stata effettuata la revisione del processo di abilitazione/disabilitazione degli utenti al fine di effettuare un migliore controllo sul ciclo di vita delle identità e sulla modifica dei relativi profili.

Le misure adottate al fine di garantire l'integrità e la disponibilità dei dati vengono di seguito elencate:

- ✓ revisione completa dell'allacciamento dei server agli UPS e alla linea elettrica;
- ✓ revisione completa dei profili necessari e sufficienti per i trattamenti a cui sono preposti;
- ✓ adeguamento degli applicativi per l'utilizzo di protocolli più sicuri;
- ✓ aggiornamento/sostituzione degli applicativi non sufficientemente stabili;
- ✓ predisposizione di un piano di formazione periodica per gli utenti e formazione al primo ingresso;
- ✓ revisione delle misure di sicurezza rispetto ai possibili danni che possono causare gli utenti che si collegano alla rete provinciale, sia verso l'infrastruttura interna che per quanto riguarda le ripercussioni all'esterno;
- ✓ completamento dell'implementazione della politica di firewalling.

Restano invece da completare le seguenti misure:

- ✓ completamento del sistema di gestione e conservazione dei log;
- ✓ revisione della configurazione delle connessioni wireless.

Criteri e modalità di ripristino della disponibilità dei dati (19.5)

I criteri per il ripristino dei dati al fine di garantirne la disponibilità, sono descritti nell'Allegato D e sono comprensivi delle politiche di salvataggio.

Interventi formativi (19.6)

Sono previsti interventi formativi per i responsabili e gli incaricati del trattamento, finalizzati a diffondere una più concreta attenzione relativamente alla tutela dei dati, con particolare riguardo a:

- ✓ profili generali della disciplina sulla protezione dei dati personali con particolare riferimento al regime delle responsabilità;
- ✓ rischi che incombono sui dati;
- ✓ misure disponibili per prevenire eventi dannosi;
- ✓ modalità per aggiornarsi sulle misure di sicurezza adottate dal titolare.

Tali interventi formativi sono programmati al verificarsi di una delle seguenti circostanze:

- ✓ al momento dell'ingresso in servizio;
- ✓ in occasione di cambiamenti di mansioni, che implichino modifiche rilevanti rispetto al trattamento di dati personali;
- ✓ in occasione della introduzione di nuovi significativi strumenti, che implichino modifiche rilevanti nel trattamento di dati personali.

Gli interventi formativi avvengono a cura delle strutture interne preposte, che si possono avvalere di personale interno o di altri soggetti esterni esperti della materia.

Trattamenti di dati personali effettuati con strumenti cartacei

I supporti cartacei, compresi quelli contenenti immagini, vengono ordinatamente raccolti in schedari, ovvero nella pratica a cui si riferiscono, per essere archiviati, una volta terminato il ciclo lavorativo, come segue:

✓ gli archivi contenenti dati sensibili e giudiziari sono localizzati in tutte le aree in cui si raccolgono le pratiche e gli schedari, ma sono conservati in armadi o cassetti chiusi a chiave;

✓ gli archivi contenenti dati personali sono collocati presso tutti gli uffici. Sono adottate idonee cautele atte a garantire la riservatezza degli interessati, quali la custodia dei documenti all'interno di fascicoli privi di indicazioni anagrafiche, anche se non necessariamente i fascicoli sono chiusi in contenitori muniti di chiave.

In generale, al personale vengono inoltre fornite le seguenti indicazioni:

✓ ridurre per quanto possibile l'utilizzo di supporti documentari cartacei;

✓ procedere alla distruzione di supporti documentari (cartacei e non) non confluiti in pratiche o istruttorie e costituenti meri strumenti di lavoro, se contenenti dati personali;

✓ ridurre al minimo la conservazione di supporti digitali al di fuori degli applicativi gestionali, se contenenti dati personali;

✓ ridurre al minimo fino ad eliminare la presenza di dati personali in documenti oggetto di pubblicazione.

Trattamenti affidati all'esterno (19.7)

La Provincia di Reggio Emilia stipula specifici atti con soggetti esterni alla propria struttura per affidare il trattamento pur rimanendo titolare dei dati, stabilendo la conformità del trattamento dei dati alla normativa vigente in materia.

Dichiarazioni d'impegno

Il presente documento viene custodito presso l'ufficio del dirigente del Servizio Bilancio, a cui afferisce l'UO Sistemi Informativi per essere esibito in caso di controlli. Viene inoltre reso pubblico sul sito istituzionale dell'Ente nelle sue parti non riservate.

Una sua copia verrà consegnata a chiunque ne faccia richiesta, in relazione all'instaurarsi di un rapporto che implichi un trattamento congiunto di dati personali.

Allegati

- Allegato A: Elenco dei procedimenti amministrativi;
- Allegato B: Elenco dei trattamenti dei dati personali e delle misure di protezione;
- Allegato C: Analisi dei rischi;
- Allegato D: Politica backup e ripristino dati;
- Allegato E: Politica di firewalling;
- Allegato F: Procedure di emergenza.