Provincia di Modena

IL PRESIDENTE

Atto numero 15 del 25/01/2021

OGGETTO: REGOLAMENTO EUROPEO UE/2016/679 O GDPR (GENERAL DATA PROTECTION REGULATION) - APPROVAZIONE E ADOZIONE DEL MODELLO DI GESTIONE INCIDENTI DI SICUREZZA E DEL DISCIPLINARE PER L'USO DEI SISTEMI INFORMATIVI NELLA PROVINCIA DI MODENA (DATA BREACH). ADOZIONE DEI CRITERI PER LA VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI.

Il 25 maggio 2018 è entrato in vigore il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (di seguito GDPR) il quale ha abrogato la direttiva 95/46/CE.

Il GDPR detta una complessa disciplina di carattere generale in materia di protezione dei dati personali, prevedendo molteplici obblighi ed adempimenti a carico dei soggetti che trattano dati personali, ivi comprese le pubbliche amministrazioni.

Il GDPR individua inoltre diversi attori che intervengono nei trattamenti di dati personali effettuati dalle organizzazioni, ciascuno con funzioni e compiti differenti.

Il D.lgs. n. 196/2003 "Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE", capo IV, art. 2 quaterdecies, come modificato dal D.lgs. 101/2018, stabilisce che il titolare del trattamento può prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate che operano sotto la propria autorità e che il titolare del trattamento individua le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta.

Il Garante della Privacy con proprio Provvedimento del 30 luglio 2019 ha fornito alle amministrazioni le modalità e i dati necessari da trasmettere ai fini della notifica in caso di violazioni dei dati personali.

Richiamati inoltre:

- gli artt. 32 e 33 del GDPR che dispongono rispettivamente che devono essere approntate misure tecniche e organizzative adeguate per garantire un livello adeguato di sicurezza dei dati personali e che in caso di violazione dei dati personali, il titolare deve notificare tale violazione all'Autorità di controllo competente senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza;
- le "Linee Guida sulla notifica delle violazioni dei dati personali ai sensi de regolamento (UE) 2016/679", adottate il 3 ottobre 2017, poi emendate ed adottate in data 6 febbraio 2018 dal

Gruppo di lavoro articolo 29 per la protezione dei dati personali (cioè l'organo consultivo indipendente dell'UE per la protezione dei dati personali e della vita privata) nelle quali vengono forniti dettagli sugli obblighi di notifica e di comunicazione delle violazioni sanciti dal GDPR, nonché alcune misure che i titolari del trattamento possono adottare per soddisfare i nuovi obblighi;

Considerato che in tema di sicurezza del trattamento dei dati personali il GDPR stabilisce che le misure tecniche ed organizzative adottate dal Titolare del trattamento devono poter garantire un livello di sicurezza adeguato al rischio, tenuto conto di:

- stato dell'arte e costi di attuazione;
- natura, oggetto, contesto e finalità di trattamento;
- rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche;
- nella valutazione dei livelli di sicurezza occorre tener conto dei rischi del trattamento derivanti da: distruzione, perdita, modifica, divulgazione non autorizzata, accesso accidentale o illegale ai dati personali trasmessi, conservati o comunque trattati;
- nel caso di violazione di dati personali (c.d. data breach), il Titolare dovrà procedere alla sua notifica al Garante, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui viene rilevata, previa valutazione dei rischi per i diritti e le libertà degli interessati.

Dato atto che la corretta gestione degli incidenti di sicurezza permette di evitare o minimizzare la compromissione dei dati dell'Ente in caso di incidente; permette inoltre, attraverso l'analisi e la comprensione dei meccanismi di attacco e delle modalità utilizzate per la gestione dell'incidente, di migliorare continuamente la capacità di risposta agli incidenti.

Dato atto, inoltre, che la nuova normativa europea fa carico alle Pubbliche Amministrazioni di non limitarsi alla semplice osservanza di un mero adempimento formale in materia di privacy, conservazione e sicurezza dei dati personali, ma attua un profondo mutamento culturale e concettuale con un rilevante impatto organizzativo da parte dell'Ente nell'ottica di adeguare le norme di protezione dei dati ai cambiamenti determinati dalla continua evoluzione delle tecnologie (cloud computing, digitalizzazione, social media, cooperazione applicativa, interconnessione di banche dati, pubblicazione automatizzata di dati on line) nelle amministrazioni pubbliche.

Ritenuto, pertanto, necessario realizzare un "modello organizzativo" sulla base di una preliminare analisi dei rischi e di un'autovalutazione finalizzata all'adozione delle migliori strategie volte a presidiare i trattamenti di dati effettuati, abbandonando l'approccio meramente formale del D.Lgs. 196/2003, limitato alla mera adozione di una lista "minima" di misure di sicurezza, realizzando, piuttosto, un sistema organizzativo caratterizzato da un'attenzione multidisciplinare alle specificità della struttura e della tipologia di trattamento, sia dal punto di vista della sicurezza informatica e in conformità agli obblighi di legge, sia in considerazione della gestione dei dati trattati. Tutto questo prevedendo, al contempo, non solo l'introduzione di nuove figure che dovranno presidiare i processi organizzativi interni per garantire un corretto trattamento dei dati personali, tra cui ad es. la figura del Responsabile della Protezione dei dati personali (RPD), ma altresì l'adozione di nuove misure tecniche ed organizzative volte a garantire l'integrità e la riservatezza dei dati, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento, la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico, nonché la verifica e la valutazione dell'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Ritenuto necessario quindi adottare uno specifico documento che, tenuto conto dell'organizzazione dell'Ente, disciplini all'interno del Provincia l'uso dei sistemi informativi e fornisca indicazioni tecniche ed organizzative da applicare per garantire la sicurezza dei dati trattati con strumentazioni informatiche, nonché uno specifico documento che in caso di incidenti di sicurezza, informatica e non, che possono occorrere ai servizi e ai dati gestiti dal Provincia, ne regolamenti la gestione.

Visto l'allegato "Disciplinare per l'uso dei sistemi informativi nel Provincia di Modena" (all. A) volto a fornire una disciplina sull'uso dei sistemi informativi che si propone anche lo scopo di impedire, o comunque ridurre, il rischio che eventuali problemi di sicurezza su una postazione o

su un punto della rete si propaghino sfruttando l'interconnettività e l'interdipendenza fra le componenti del sistema informativo del Provincia.

Visto inoltre l'allegato modello di gestione degli incidenti di sicurezza (All. B) che, oltre a prevedere la costituzione di una struttura operativa competente (c.d. "gruppo per la Gestione della Sicurezza ICT") in grado di intervenire secondo le procedure operative prestabilite, individua, con specifico riferimento all'obbligo di cui all'art. 33 del GDPR n. 679/2016:

- le violazioni dei dati personali (c.d. data breach) che ricadono nell'ambito della normativa in materia di protezione dei dati, tenendo conto del fatto che tutte le violazioni dei dati personali sono incidenti di sicurezza, ma non tutti gli incidenti di sicurezza sono necessariamente violazioni di dati personali;
- i casi in cui l'Ente deve notificare i data breach al Garante ed agli interessati;
- le misure atte a trattare il rischio e la documentazione da produrre.

Valutato che la struttura operativa deputata ad intervenire secondo le procedure operative prestabilite (c.d. "gruppo per la Gestione della Sicurezza ICT") debba essere costituita dalle seguenti figure:

- il Responsabile dell'u.o. "Informatica, Sistemi e reti";
- il Responsabile dell'u.o. "Analisi e programmazione sistemi gestionali;
- il Direttore dell'Area Amministrativa in quanto incaricato quale dirigente del Servizio Personale e sistemi informativi e telematica.
- il Responsabile di Servizio nell'ambito del quale si è verificato la violazione;
- eventuali altri soggetti coinvolti nel trattamento dei dati oggetto di violazione che il gruppo riterrà necessario interessare a seconda della tipologia di incidente e della tipologia di dati coinvolti.

Ritenuto, infine, in attuazione dell'art. 33, paragrafo 5, del GDPR (il quale prevede che il titolare del trattamento "documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per provi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo") ed in ossequio al principio di accountability come suggerito dalla Linee guida in materia adottate dal Gruppo di lavoro articolo 29 per la protezione dei dati, di istituire un registro interno delle violazioni in cui documentare tutte le violazioni, sia quelle notificabili che non notificabili, da tenere a cura del Direttore dell'Area Amministrativa, nella sua funzione di componente del Gruppo per la Gestione della sicurezza.

Visti:

- il D.Lgs. n. 267/2000;
- il GDPR 2016/679, ed in particolare gli artt. 32, 33 e 34 del Regolamento europeo;
- il D.Lgs. n. 196/2003, nel testo integrato con le modifiche introdotte dal D.Lgs. n. 101/2018;
- le "Linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679", adottate il 3 ottobre 2017 ed emendate ed adottate in data 6 febbraio 2018 dal Gruppo di lavoro articolo 29 per la protezione dei dati.

Il Responsabile del procedimento è il Direttore dell'Area Amministrativa, Dr. Raffaele Guizzardi.

Si informa che il titolare del trattamento dei dati personali forniti dall'interessato è la Provincia di Modena, con sede in Modena, viale Martiri della Libertà 34, e che il Responsabile del trattamento dei medesimi dati è il Direttore dell'Area Amministrativa

Le informazioni che la Provincia deve rendere ai sensi dell'art. 13 del D.lgs. 196/2003 ed in attuazione del Regolamento UE 679/2016 sono contenute nel "Documento Privacy", di cui l'interessato potrà prendere visione presso la segreteria dell'Area Amministrativa della Provincia di Modena e nel sito internet dell'Ente www.provincia.modena.it.

Il presente atto non comporta riflessi diretti o indiretti sulla situazione economico-finanziaria o sul patrimonio dell'ente.

Il Dirigente responsabile del Servizio interessato ha espresso parere favorevole in ordine alla regolarità tecnica in relazione al presente atto.

Per quanto precede,

IL PRESIDENTE DISPONE

1) di approvare il "Disciplinare per l'uso dei sistemi informativi della Provincia di Modena", allegato al presente atto quale parte integrante e sostanziale (all. "A"), volto a impedire o, comunque, a ridurre, il rischio del verificarsi di problemi di sicurezza;

2) di approvare, in attuazione degli adempimenti previsti dal Regolamento Europeo UE/2016/679, il "Modello di gestione degli incidenti di sicurezza (Manuale Data Breach)", allegato al presente atto quale parte integrante e sostanziale (all. "B") che definisce le procedure che la Provincia di Modena deve adottare in caso di violazione dei dati personali;

3) di disporre, contestualmente all'approvazione, l'immediata adozione da parte dell'Ente del suddetto modello che prevede, tra l'altro, la costituzione di una struttura operativa (c.d. "Gruppo per la Gestione della Sicurezza ICT") deputata ad intervenire in caso di incidente di sicurezza secondo le procedure operative prestabilite e costituita, di volta in volta, dalle seguenti figure:
   - il Responsabile dell'u.o. "Informatica, Sistemi e reti";
   - il Responsabile dell'u.o. "Analisi e programmazione sistemi gestionali"
   - il Direttore dell'Area Amministrativa in quanto incaricato quale dirigente del Servizio Personale e sistemi informativi e telematica.
   - il Responsabile di Servizio nell'ambito del quale si è verificato la violazione;
   - eventuali altri soggetti coinvolti nel trattamento dei dati oggetto di violazione che il gruppo riterrà necessario interessare a seconda della tipologia di incidente e della tipologia di dati coinvolti;

4) di confermare i Direttori delle Aree quali Responsabili del trattamento dei dati della Provincia di Modena, secondo quanto già disposto nell'atto del Presidente n. 75 del 30/5/2018;

5) di designare tutti i dipendenti della Provincia di Modena, come incaricati del trattamento dei dati personali effettuato nello svolgimento delle proprie funzioni in riferimento alle attività contenute nel PEG 2020/2022 approvato con atto del Presidente n.18 del 13/02/2020. I responsabili del trattamento dei dati sono autorizzati a nominare, nel rispetto della normativa e nell'ambito delle proprie prerogative, anche personale esterno, quale incaricato al trattamento dei dati;

6) di disporre, in attuazione dell'art. 33, paragrafo 5, del GDPR e delle "Linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679" adottate dal Gruppo di lavoro articolo 29 per la protezione dei dati, in ossequi al principio di accountability, la tenuta di un apposito "Registro delle violazioni di dati personali" secondo il modello allegato (all. "C") a cura del Responsabile dell'Area Amministrativa;

7) di adottare i criteri propedeutici al fine dell'analisi dei trattamenti da sottoporre alla valutazione d'impatto (all. "D");

8) di trasmettere il presente atto al RPD della Provincia di Modena per la verifica della coerenza del "Modello di gestione degli incidenti di sicurezza" approvato con i principi del GDPR, impegnandosi a recepire eventuali osservazioni e integrazioni che dovessero pervenire da parte del medesimo;

9) di pubblicare sul sito web dell'Ente, in apposita sezione, il presente atto, unitamente alla indicazione dei riferimenti di contatto del "Gruppo per la Gestione della Sicurezza ICT" nonché della procedura da attivare in caso di sospetta violazione di dati personali.

Il Presidente
TOMEI GIAN DOMENICO

(Sottoscritto digitalmente ai sensi
dell'art. 21 D.L.gs n 82/2005 e s.m.i.)