

DECRETO DEL DIRETTORE DELLA DIREZIONE ICT E AGENDA DIGITALE n. 119 del 26 settembre 2018

Adozione delle Linee Guida per la notifica della violazione dei dati personali ("Data Breach") e della relativa modulistica, in attuazione degli artt. 33 e 34 del Regolamento (UE) 2016/679 recante "Regolamento Generale sulla Protezione dei Dati (GDPR)" e della DGR n. 596 del 08/05/2018.

[Informatica]

Note per la trasparenza:

Con il presente provvedimento il Direttore della Direzione ICT e Agenda Digitale provvede ad adottare le *"Linee Guida per la notifica della violazione dei dati personali (Data Breach)"* (**Allegato A**) e la relativa modulistica (**Allegato B**), in attuazione della DGR n. 596 del 08/05/2018 e conformemente alle prescrizioni indicate agli artt. 33 e 34 del *Regolamento Generale sulla Protezione dei Dati (GDPR)* approvato con Regolamento (UE) 2016/679, adottato in data 27/04/2016 dal Parlamento Europeo e dal Consiglio dell'Unione Europea, così come attuato con DGR n. 596 del 08/05/2018.

Il Direttore

Premesso che:

- in data 27/04/2016 il Parlamento Europeo ed il Consiglio dell'Unione Europea hanno adottato il Regolamento (UE) 2016/679 recante *"Regolamento Generale sulla Protezione dei Dati - GDPR"*, il quale detta la normativa sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali tipologie di dati;

- il Regolamento (UE) 2016/679 ha trovato applicazione a decorrere dal 25/05/2018, data in cui i soggetti pubblici e gli Stati membri che trattano dati personali sono stati tenuti a darvi attuazione, anche in mancanza di una legislazione statale o regionale specifica. Per effetto di tale nuova normativa europea, la protezione dei dati personali ha subito un profondo rinnovamento;

- la principale novità introdotta dal predetto Regolamento Europeo è rappresentata dal principio della "responsabilizzazione" (*"accountability"*) che attribuisce al Titolare e, più in generale, a chi tratta dati personali il compito di mettere in atto *"misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al regolamento"*.

Atteso che:

- in applicazione del suddetto Regolamento, con DGR n. 473 del 10/04/2018 è stato designato il Responsabile della Protezione dei Dati Personali (*D.P.O.*) mentre con DGR n. 596 del 08/05/2018 sono state adottate misure attuative relativamente alla protezione dei dati personali e sono state impartite istruzioni per i trattamenti dei medesimi dati;

- con il suddetta DGR n. 596/2018 il Direttore della Direzione ICT e Agenda Digitale è stato delegato all'adozione, gestione ed implementazione delle soluzioni tecnico-informatiche atte a prevenire e contrastare i rischi connessi alla sicurezza informatica (*c.d. cyber-security*) correlati alla protezione dei dati personali, con conseguenti funzioni gestionali ed operative;

- la Direzione ICT e Agenda Digitale, sempre in ottemperanza al citato provvedimento della Giunta regionale, fa stabilmente parte del *"Gruppo di Lavoro GDPR"* che svolge compiti operativi, di gestione, supporto, analisi e soluzione dei problemi applicativi del Regolamento in oggetto.

Posto che:

- per le violazioni di dati personali (che comportano «accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati») il citato GDPR stabilisce, all'articolo 33, paragrafo 1, che: *"in caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente [...] senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo"*; Si intendono oggetto dell'eventuale obbligo di notifica anche i *"databreach"* avvenuti presso i responsabili "esterni" o loro eventuali sub-responsabili (per quanto attinente ai trattamenti di dati affidati);

- come disposto dalla predetta deliberazione attuativa n. 596/2018, il Direttore della Direzione ICT e Agenda Digitale (sulla base degli esiti dell'istruttoria condotta da ciascun Delegato al Trattamento) è stato incaricato di notificare al Garante per la Protezione dei dati personali il databreach, per conto del Titolare del trattamento senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, informandone contestualmente il Data Protection Officer (D.P.O.);

- inoltre l'articolo 34 del GDPR si occupa della questione della necessità di avvisare o meno l'interessato circa l'avvenuto databreach, stabilendo che quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, è obbligatorio comunicare la violazione all'interessato senza ingiustificato ritardo, salvo eccezioni.

Considerato che:

- al fine di ottemperare agli obblighi predetti, è necessario che tutte le persone autorizzate al trattamento siano adeguatamente istruite affinché trattino correttamente i dati personali e informino, con la massima celerità, il Delegato di ogni violazione rilevata (databreach), affinché possa procedere con le dovute segnalazioni;

- a tal scopo, si adottano in allegato al presente provvedimento le "*Linee Guida per la notifica della violazione dei dati personali ("Data Breach")*" ai sensi degli artt. 33 e 34 del citato Regolamento (UE) 2016/679 (**Allegato A**) ed il relativo "*Modulo per la notifica della violazione dei dati personali (Data Breach)*" (**Allegato B**), entrambi parti integranti e sostanziali dello stesso.

TUTTO CIÒ PREMESSO

- VISTO il Decreto Legislativo n. 196 del 30/06/2003 "*Codice in materia di protezione dei dati personali*";

- VISTO il Regolamento (UE) 2016/679, in particolare gli artt. 33 e 34;

- VISTO il Regolamento Regionale n. 1 del 24/10/2014, emanato ai sensi degli artt. 20, co. 2 e 21, co. 2 del D.Lgs. n. 196/2003;

- VISTE la DGR n. 473 del 10/04/2018 e la DGR n. 596 del 08/05/2018.

decreta

1. di adottare - quale **Allegato A** al presente provvedimento - le "*Linee Guida per la notifica della violazione dei dati personali ("Data Breach")*", ai sensi degli artt. 33 e 34 del Regolamento (UE) 2016/679 recante "*Regolamento Generale sulla Protezione dei Dati - GDPR*";
2. di adottare - quale **Allegato B** al presente atto - il relativo "*Modulo per la notifica della violazione dei dati personali (Data Breach)*", ai sensi dell'art. 33 del Regolamento (UE) 2016/679;
3. di dare atto che il presente decreto non comporta spesa a carico del bilancio regionale;
4. di dare atto che il presente provvedimento (e relativi allegati) sarà pubblicato nell'intranet regionale all'indirizzo: http://www.regione.veneto.it/web/informatica-e-e-government/informativa_privacy;
5. di pubblicare integralmente il presente decreto nel Bollettino Ufficiale della Regione.

Idelfo Borgo