



REGIONE DEL VENETO

giunta regionale

DECRETO N. 116 DEL 29/10/2019

OGGETTO: Attuazione dell'art. 33 del Regolamento (UE) 2016/679 "Regolamento Generale sulla Protezione dei Dati (GDPR)" e della DGR n. 596 del 08/05/2018. Adozione del documento denominato "Modulo per la notifica della violazione dei dati personali ("Data Breach")" in sostituzione dell'analogo modulo già approvato con DDR n. 119 del 26/09/2018.

STRUTTURA DIREZIONE ICT E AGENDA DIGITALE

Trattasi di atto:

- che comporta assunzione di impegno di spesa
- che contiene termini o scadenze
- che comprende allegati

x il presente decreto è soggetto a pubblicazione integrale nel BURV.

Venezia,

**P. O. Gestione Giuridico
Amministrativa dei rapporti
con i fornitori in ambito ICT
dott. Riccardo Zeggio**

Barrare le caselle che interessano

Inviato in Ragioneria

Restituito

Si invia alla struttura proponente, per l'esecuzione

Venezia,

IL DIRETTORE DELLA
DIREZIONE ICT E AGENDA DIGITALE

dott. Idelfo Borgo

Eventuali note:



REGIONE DEL VENETO

giunta regionale

DECRETO N. 116 DEL 29/10/2019

OGGETTO: Attuazione dell'art. 33 del Regolamento (UE) 2016/679 "*Regolamento Generale sulla Protezione dei Dati (GDPR)*" e della DGR n. 596 del 08/05/2018. Adozione del documento denominato "*Modulo per la notifica della violazione dei dati personali ("Data Breach")*" in sostituzione dell'analogo modulo già approvato con DDR n. 119 del 26/09/2018.

NOTE PER LA TRASPARENZA:

Con il presente provvedimento si adotta - quale **Allegato A** - il documento denominato "*Modulo per la notifica della violazione dei dati personali (Data Breach)*" ai sensi dell'art. 33 del Regolamento (UE) 2016/679, il quale sostituisce integralmente l'analogo modulo già approvato con DDR n. 119 del 26/09/2018 del Direttore della Direzione ICT e Agenda Digitale, al fine di uniformarsi al modello di notifica introdotto con provvedimento n. 157 del 30/07/2019 del Garante per la protezione dei dati personali.

IL DIRETTORE DELLA

DIREZIONE ICT E AGENDA DIGITALE

Premesso che:

- il Parlamento Europeo e il Consiglio dell'Unione Europea hanno adottato, in data 27/04/2016, il Regolamento (UE) 2016/679 recante "*Regolamento Generale sulla Protezione dei Dati - GDPR*" il quale detta la normativa sulla protezione delle persone fisiche circa il trattamento dei dati personali e la 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*";
- con l'espressione «*violazione dei dati personali*» si intende la violazione di sicurezza che comporta (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 (*vd. art. 4, punto 12 del Regolamento*);

Atteso che:

- in applicazione del suddetto Regolamento, con DGR n. 473 del 10/04/2018 la Regione del Veneto ha 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 operative per i trattamenti degli stessi;
- la citata DGR n. 596/2018 ha altresì delegato il Direttore della Direzione ICT e Agenda Digitale all'adozione, gestione ed implementazione delle soluzioni tecnico-informatiche atte a prevenire/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.

Mod. A - originale

Posto che:

- i Titolari di trattamento di dati personali sono tenuti a notificare al Garante le violazioni dei medesimi dati (*data breach*) che comportano (accidentalmente o in modo illecito) la distruzione, la perdita, la modificazione, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati, anche nell'ambito delle comunicazioni elettroniche, a meno che sia improbabile che la violazione presenti un rischio per i diritti e le libertà degli interessati;
- in particolare, per le succitate violazioni di dati personali il GDPR stabilisce, all'art. 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 n. 72 ore, è corredata dei motivi del ritardo*". Si puntualizza che vengono considerati oggetto dell'eventuale obbligo di notifica anche i "*data breach*" avvenuti presso i responsabili "esterni" o i 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 per gli aspetti di propria competenza) è stato incaricato di notificare il *data breach* al Garante per la protezione dei dati personali, per conto del Titolare del trattamento. Tale notifica deve avvenire 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.);
- peraltro l'art. 34 del GDPR si occupa della questione della necessità di avvisare o meno l'interessato circa l'avvenuto *data breach*, stabilendo che quando la violazione dei dati personali sia 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 di notifica imposti dall'art. 33 del GDPR, con DDR n. 119 del 26/09/2018 la Direzione ICT e Agenda Digitale ha adottato uno specifico modulo per la notifica delle violazioni dei dati personali (*Data Breach*), il cui testo e' stato pubblicato sia sul BURV n. 100 del 05/10/2018 che nell'intranet regionale;
- con provvedimento n. 157 del 30/07/2019 il Garante per la protezione dei dati personali ha introdotto un nuovo modello ufficiale contenente le informazioni minime necessarie per notificare una violazione di dati personali ai sensi dell'art. 33 del GDPR, razionalizzando e uniformando i termini, i contenuti e le modalità della notifica;
- al fine di uniformarsi alla nuova modulistica approvata dal Garante per la protezione dei dati personali risulta allo stato opportuno sostituire il modulo per la notifica dei *Data Breach* ai sensi dell'art. 33 del Regolamento (UE) 2016/679, già approvato con DDR n. 119 del 26/09/2018 del Direttore della Direzione ICT e Agenda Digitale;
- alla luce di quanto sopra, si approva come parte integrante e sostanziale del presente provvedimento il documento denominato "*Modulo per la notifica della violazione dei dati personali (Data Breach)*" - **Allegato A**.
Tale documento è conforme ai contenuti minimi necessari per notificare una violazione di dati personali definiti dal provvedimento n. 157 del 30/07/2019 il Garante per la protezione dei dati personali.

TUTTO CIÒ PREMESSO

- VISTO il Regolamento (UE) 2016/679, in particolare gli artt. 33 e 34;
- VISTO il D.Lgs. n. 196 del 30/06/2003 "*Codice in materia di protezione dei dati personali*" così come modificato dal D.Lgs. n. 101 del 10/08/2018;
- VISTO il Regolamento Regionale n. 1 del 24/10/2014, emanato ai sensi degli artt. 20, comma 2 e 21, comma 2 del D.Lgs. n. 196/2003;
- VISTO il D.Lgs. n. 51 del 18/05/2018, recante "*Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati*";
- RICHIAMATE la DGR n. 473 del 10/04/2018 e la DGR n. 596 del 08/05/2018;
- VISTO il DDR n. 119 del 26/09/2018 e il relativo Allegato B "*Modulo per la notifica della violazione dei dati personali (Data Breach)*";

- VISTO il provvedimento n. 157 del 30/07/2019 del Garante per la protezione dei dati personali relativo alla notifica delle violazioni dei dati personali (*data breach*) e la modulistica dallo stesso richiamata.

DECRETA

1. di prendere atto che con provvedimento n. 157 del 30/07/2019 il Garante per la protezione dei dati personali ha introdotto un nuovo modello ufficiale contenente le informazioni “minime” necessarie al fine di effettuare la notifica di una violazione di dati personali (*Data Breach*) ai sensi dell’art. 33 del Regolamento (UE) 2016/679 (*GDPR*);
2. di adottare, al fine di conformarsi alle indicazioni di cui al citato provvedimento n. 157/2019 del Garante, il documento denominato “*Modulo per la notifica della violazione dei dati personali (Data Breach)*” ai sensi dell’art. 33 del Regolamento (UE) 2016/679, il quale si approva come parte integrante e sostanziale del presente provvedimento - **Allegato A**;
3. di dare atto che il documento di cui all’**Allegato A** sostituisce integralmente l’analogo modulo già approvato con DDR n. 119 del 26/09/2018 del Direttore della Direzione ICT e Agenda Digitale;
4. di dare atto che il presente decreto non comporta spesa a carico del bilancio regionale;
5. 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;
6. di pubblicare integralmente il presente decreto nel Bollettino Ufficiale della Regione.

Il Direttore
dott. ~~Renzo~~ Borgo



P. O. Gestione Giuridico
Amministrativa dei rapporti
con i fornitori in ambito ICT
dott. Riccardo Zeggio