REGIONE MARCHE
Giunta regionale

DECRETO DEL DIRETTORE DELLA AGENZIA REGIONALE SANITARIA
n. 67 del 24 ottobre 2022

Oggetto: REGOLAMENTO (UE) 2016/679 - Approvazione procedura per la gestione dei data breach e istituzione Registro databreach.

VISTO il documento istruttorio e ritenuto, per le motivazioni nello stesso indicate, di adottare il presente decreto;

VISTO l'art. 15 della L.R. n. 18 del 30/07/2021 "Disposizioni di organizzazione e di ordinamento del personale della Giunta regionale";

DECRETA

1. Di approvare la procedura, per la gestione della violazione dei dati personali (DATA BREACH),contenente le indicazioni, le responsabilità e la descrizione delle azioni da attuare per la gestione della procedura da attivare in caso di possibile violazione dei dati personali, in osservanza agli obblighi relativi alla notifica all'Autorità Garante per la protezione dei dati personali e alla comunicazione all'interessato, in ossequio alle previsioni di cui agli articoli 33 e 34 del Regolamento europeo n. 679 del 2016, così come descritta nell'Allegato A, ivi compresi i relativi allegati n.1, n. 2, n.3, n.4 e 5, parte integrante e sostanziale del presente decreto;
2. Di stabilire che è tenuto al rispetto della procedura tutto il personale operante, a qualsiasi titolo(dipendente, in comando, distacco e utilizzo) presso l'Agenzia Regionale Sanitaria nonchè tutti i soggetti esterni (persona fisica o persona giuridica) che, in ragione del rapporto contrattuale in essere con il Titolare del trattamento,agisca in qualità di Responsabile del trattamento (art. 28 GDPR);
3. Di stabilire che la proceduta di data breach sarà supportata da sessioni formative, di concerto con il DPO, al fine di formare e responsabilizzare al meglio il personale, nel rispetto del principio di *Accountability*;
4. Di disporre che al presente provvedimento venga assicurata:

   - la pubblicità legale con pubblicazione, per estratto, sul B.U.R della Regione Marche;

   - la trasparenza mediante la pubblicazione sul sito web istituzionale, nella sezione "*Amministrazione trasparente*", sezione di primo livello "*Disposizioni generali*" sezione di secondo livello "*Atti generali*;

   - la massima diffusione presso tutto il personale operante, a qualsiasi titolo(dipendente,in comando, distacco e utilizzo) presso l'Ente e presso tutti i soggetti esterni qualificabili in

termini di responsabili del trattamento;

5. di dare atto che le disposizioni operative sono assoggettate a revisione ogni qualvolta si renderà necessario;

Si attesta l'avvenuta verifica della inesistenza di situazioni anche potenziali di conflitto di interesse ai sensi dell'art. 6 bis della Legge 241/1990 e s.m.i.

Per Il Direttore
(Armando Marco Gozzini)
Paolo Aletti

Documento informatico firmato digitalmente

REGIONE MARCHE
Giunta regionale

DOCUMENTO ISTRUTTORIO

NORMATIVA DI RIFERIMENTO

- Legge 241/1990;
- D.Lgs. 196/2003;
- Legge 190/2012;
- D.Lgs. 33/2013;
- Regolamento (UE) n. 679/2016;
- art. 4, comma 2, L.R. 26/96 e ss.mm.ii;
- Dichiarazioni del gruppo di lavoro articolo 29 sulla protezione dei dati (WP29) - 14/EN;
- Linee-guida sui responsabili della protezione dei dati (RPD) - WP243 Adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;
- Linee-guida sul diritto alla "portabilità dei dati" - WP242 Adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;
- Linee-guida per l'individuazione dell'autorità di controllo capofila in rapporto a uno specifico titolare o responsabile del trattamento - WP244 adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;
- Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679 - WP248 adottate dal Gruppo di lavoro Art. 29 il 4 aprile 2017;
- Linee guida elaborate dal Gruppo Art. 29 in materia di applicazione e definizione delle sanzioni amministrative - WP253 adottate dal Gruppo di lavoro Art. 29 il 3 ottobre 2017;
- Linee guida elaborate dal Gruppo Art. 29 in materia di processi decisionali automatizzati e pro lazione - WP251 Adottate dal Gruppo di lavoro Art. 29 il 6 febbraio 2018;
- Linee guida elaborate dal Gruppo Art. 29 in materia di notifica delle violazioni di dati personali (data breach notification) - WP250 Adottate dal Gruppo di lavoro Art. 29 il 6 febbraio 2018;
- Parere del WP29 sulla limitazione della finalità - 13/EN WP 203;
- il Provvedimento del Garante sulla notifica delle violazioni dei dati personali (data breach) - 30 luglio 2019 [doc-web n. 9126951];

MOTIVAZIONE

La protezione delle persone fisiche, con riguardo al trattamento dei dati di carattere personale, è un diritto fondamentale dal momento che l'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea («Carta») e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea («TFUE») riconoscono ad ogni persona il diritto alla protezione dei dati di carattere personale che la riguardano.

Le modalità di protezione dei dati personali devono confrontarsi con la rapidità dell'evoluzione tecnologica e della globalizzazione, considerando, in particolare che:

- la portata della condivisione e della raccolta di dati personali è aumentata in modo significativo;
- la tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività;
- la tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali.

L'Unione europea, con 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 e che abroga la direttiva 95/46/CE (di seguito solo "GDPR"), ha predisposto un impianto normativo solido e coerente per la tutela dei dati personali, in risposta alla rapidità dell'evoluzione tecnologica e alla globalizzazione.

Dato atto che il 24 maggio 2016 è entrato ufficialmente in vigore il GDPR, il quale è diventato definitivamente applicabile in via diretta in tutti i Paesi UE a partire dal 25 maggio 2018.

Ciò premesso per «*violazione dei dati personali*» (data breach) 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 (*art. 4, punto 12 del Regolamento; art. 2, comma 1, lett. m, del D.lgs. n. 51/2018*).

In caso di violazione dei dati personali, il titolare del trattamento è tenuto a notificare tale evento al Garante 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 (*artt. 33 e 55 del Regolamento, art. 2-bis del Codice*);

il titolare del trattamento è tenuto, altresì, a notificare la violazione dei dati personali al Garante con le modalità di cui all'art. 33 del Regolamento anche con riferimento al trattamento effettuato a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, salvo che il trattamento medesimo sia effettuato dall'autorità giudiziaria nell'esercizio delle funzioni giurisdizionali, nonché di quelle giudiziarie del Pubblico Ministero (*artt. 26 e 37, comma 6, del D.lgs. n. 51/2018*).

La notifica all'autorità di controllo deve obbligatoriamente contenere almeno i seguenti elementi:

- descrizione della natura della violazione dei dati personali e le registrazioni dei dati personali in questione;

- comunicazione del nome e dei dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere maggiori informazioni;

- descrizione delle probabili conseguenze della violazione dei dati personali;

- descrizione delle misure adottate o da adottare da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi;

La stessa violazione dei dati personali, quando è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, va comunicata all'interessato senza ingiustificato ritardo.

Nello specifico tale comunicazione deve descrivere con un linguaggio semplice, chiaro e trasparente la natura della violazione dei dati personali, contenendo obbligatoriamente i seguenti contenuti minimi:

- il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto;

- una descrizione delle probabili conseguenze della violazione;

- una descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione e anche, se del caso, per attenuarne i possibili effetti negativi.

L'omessa notifica di data breach all'Autorità di controllo o l'omessa comunicazione agli interessati, nei casi in cui siano soddisfatti i requisiti di cui agli artt. 33 e 34 GDPR, comporta pesanti sanzioni amministrative (*art. 83 GDPR*), il cui importo può arrivare a 10.000.000 di euro o al 2% del fatturato

totale annuo dell'esercizio precedente, se superiore, nonché le misure correttive di cui *all'art. 58 GDPR* (avvertimenti, ammonimenti, ingiunzioni, imposizione di limiti al trattamento, ordine di rettifica, revoca di certificazioni, ordine di sospendere flussi dati).

Allo stesso modo l'art. 82 prevede che chiunque subisca un danno materiale o immateriale causato da una violazione del GDPR ha il diritto di ottenere il risarcimento del danno dal soggetto al quale l'obbligo (violato) era imposto (salvo che quest'ultimo dimostri che l'evento dannoso non gli è imputabile).

L' elemento che può sicuramente mitigare il livello sanzionatorio, a fronte di una violazione, così come previsto nello stesso GDPR, all'art. 83 paragrafo 2, è il comportamento del titolare che possa dimostrare come, intervenendo con tempismo, abbia fatto il possibile per ridurre la gravità, la natura e la durata della violazione.

L'atteggiamento reattivo e cooperativo comporta, inoltre, un'attenuazione delle sanzioni applicabili.

Rilevato che, per quanto sopra, è necessario istituire:

1. una Procedura *data breach;*

2. un registro interno *data breach*, dove vengono annotate sia le violazioni non notificabili che quelle notificabili, il quale deve contenere i seguenti dati:

- i dettagli relativi alla violazione (cause, fatti e dati personali interessati);
- gli effetti e le conseguenze della violazione;
- i provvedimenti adottati per porvi rimedio;
- il ragionamento alla base delle decisioni prese in risposta a una violazione.

In particolare, il rispetto dell'adottanda procedura è obbligatorio per tutti i soggetti che, a qualsiasi titolo, trattano dati personali di competenza del Titolare, quali:

i. i lavoratori dipendenti, nonché coloro che a qualsiasi titolo - e quindi a prescindere dal tipo di rapporto contrattuale intercorrente - abbiano accesso ai dati personali trattati nel corso delle prestazioni richieste per conto del Titolare del trattamento.
ii. qualsiasi soggetto (persona fisica o persona giuridica) diverso da quelli indicati alla lettera precedente che, in ragione del rapporto contrattuale in essere con il Titolare del trattamento abbia accesso ai suddetti dati e agisca in qualità di Responsabile del trattamento (art. 28 GDPR) o di autonomo Titolare. In particolare, ogniqualvolta il Titolare si trovi ad affidare il trattamento di dati ad un soggetto terzo, in qualità di responsabile del trattamento, è tenuta a stipulare con tale soggetto uno specifico contratto che lo vincoli al rispetto delle istruzioni impartitegli dal Titolare in materia di protezione dati: è necessario che la presente procedura di segnalazione di data breach sia inclusa nel suddetto contratto. Ciò al fine di obbligare il responsabile ad informare il Titolare del trattamento senza ingiustificato ritardo, di ogni potenziale evento di data breach;

Nel rispetto del principio di Accountability, la procedura di data breach, verrà supportata attraverso sessioni formative, di concerto con il DPO, al fine di formare e responsabilizzare al meglio il personale operante in ARS.

Si dà atto che le disposizioni operative in materia di incidenti di sicurezza e di violazione di dati personali (c.d. data breach) e loro allegati (dal n.1 al n.5) sono corrispondenti alla struttura organizzativa dell'Ente e adeguate sotto il profilo operativo alle esigenze del medesimo.

Pertanto, per quanto sopra esplicitato si rende necessario procedere all'approvazione della procedura data breach (allegato A) nonché degli allegati (dal n.1 al n.5) parte integrante e sostanziale del presente atto.

ESITO DELL'ISTRUTTORIA

Per quanto sopra esposto, si propongono le determinazioni indicate nel dispositivo.

Il sottoscritto, in relazione al presente provvedimento, dichiara, ai sensi dell'art.47 del DPR 445/2000, di non trovarsi in situazioni anche potenziali di conflitto di interesse ai sensi dell'art. 6 bis della L.241/1990 e degli artt.6 e 7 del DPR 62/2013 e della DGR 64/2014.

Il responsabile del procedimento
(Maurizio Meduri)

Documento informatico firmato digitalmente

ALLEGATI

Allegato A Procedura Data Breach;
Allegato n.1 Tipologia di Violazione;
Allegato n.2 Tipologia di Eventi;
Allegato n.3 Fattori da considerare quando si valuta il rischio;
Allegato n.4 Fac-Simile modello di notifica;
Allegato n.5 Registro Data Breach.