



Regione Piemonte - Azienda Sanitaria Locale CN2 "Alba - Bra"

O G G E T T O :

ATTUAZIONE REG. (UE) 2016/679 DEL 27.04.2016 RELATIVO ALLA PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI, NONCHÉ ALLA LIBERA CIRCOLAZIONE DI TALI DATI.

AGGIORNAMENTO PROCEDURA DATA BREACH.

I L D I R E T T O R E G E N E R A L E

nominato con Deliberazione della Giunta Regionale n. 21-651/2024/XII del 23/12/ 2024

Visti il Regolamento UE n. 2016/679, il D. Lgs. n. 101/2018 del 10.8.2018 ed il D. Lgs. n. 196/2003 del 30.6.2003 e s.m.i.;

Dato atto che:

- per "data breach" si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati,
- se l'incidente di sicurezza non coinvolge dati personali, non vi è data breach,
- un data breach può originare sia dall'esterno che dall'interno dell'Azienda, e che casi quali: un utente che modifica erroneamente un database o un malware che crittografa una cartella di rete o il semplice smarrimento di una chiavetta USB o di un telefonino aziendale, sono tutte potenziali violazioni dei dati personali;

Atteso che con Deliberazione n. 517 del 18.12.2018 veniva approvata la procedura di notifica di una violazione dei dati personali all'autorità di controllo, ai sensi dell'art. 33 del Reg. UE n. 2016/679, la c.d. "Data breach", e che con successiva Deliberazione n. 665 del 19.11.2021 provvedeva all'aggiornamento della suddetta procedura, in collaborazione tra le Aziende Sanitarie Asl Cn1 e Azienda Sanitaria Ospedaliera "S. Croce e Carle";

Considerato che il Comitato Europeo per la Protezione dei dati (EDPB) ha adottato le nuove Linee Guida 01/2021 sulla notifica di data breach, fornendo indicazioni su come gestire una violazione dati ed una analisi di casi, con una serie di esempi relativi proprio all'obbligo di notifica delle violazioni di sicurezza all'Autorità di Controllo previsto dall'art. 33 del GDPR;

Ritenuto, altresì, opportuno richiamare il provvedimento del Garante per la protezione dei dati personali n. 209 del 27.5.2021, con il quale è stata istituita una nuova procedura telematica per la notifica delle violazioni dei dati personali ex art. 33 GDPR;

Visto il predetto art. 33, che dispone: " In caso di violazione di dati personali, il Titolare del trattamento (Asl Cn2) notifica la violazione all'Autorità di controllo competente (Autorità Garante per la protezione dei dati personali)...senza ingiustificato ritardo e, ove possibile, entro le 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 ";

Atteso che in considerazione di quanto sopra e dell'evoluzione del quadro normativo europeo e nazionale in materia di sicurezza informatica, si ritiene necessario aggiornare la procedura di gestione dei data breach, al fine di garantire la piena conformità alle disposizioni sopravvenute:

Vista la Direttiva NIS2, entrata in vigore il 18 gennaio 2023, che amplia e rafforza gli obblighi di sicurezza e di risposta agli incidenti informatici per gli operatori di servizi essenziali e i fornitori di servizi digitali, includendo anche obblighi più stringenti in merito alla notifica tempestiva degli incidenti significativi, che devono essere comunicati all'autorità competente entro 24 ore dall'individuazione.

Considerato che la procedura deve essere applicata in tutti i casi in cui si verifichi sui dati personali una perdita, distruzione o diffusione indebita (ad es. a seguito di attacchi informatici, accessi abusivi, ecc...);

Atteso che tutti i soggetti dell'Organigramma Privacy dell'ASLCN2, approvato con deliberazione n. 198 del 28/03/2025, sono tenuti a comunicare tempestivamente al Titolare i casi di accesso non autorizzato ai dati o di trattamento non consentito o non conforme alle finalità istituzionali, secondo i termini e le modalità di cui alla procedura di "Data breach";

Vista la proposta di modifica della predetta procedura, proposta dal DPO ed esaminata nell'ambito del Gruppo Privacy aziendale;

Su proposta conforme del Responsabile f.f. della S.S. Affari Generali e Segreteria Organismi Collegiali – Coordinatore Gruppo Privacy aziendale (dott.ssa Tiziana ROSSINI), che attesta la legittimità nonché la regolarità formale e sostanziale di quanto innanzi indicato.

Acquisito il parere favorevole, per quanto di competenza, del Direttore Sanitario e del Direttore Amministrativo (ex art. 3, comma 1-quinquies, D.Lg.vo 30.12.92, n. 502 e s.m.i.);

D E L I B E R A

- di procedere, per le motivazioni e nei termini illustrate in premessa, all'aggiornamento della procedura specifica di "Data breach", ex art. 33 del GDPR, denominata "PGSGQ131-Revisione n. 02", ed **allegata** al presente provvedimento, in sostituzione di quella approvata con Deliberazione n. 665 del 19.11.2021;
- di dare atto che la nuova procedura di "Data breach" denominata PGSGQ131-Revisione n. 02", viene pubblicata sul sito Internet aziendale al seguente link: Procedure - Privacy - ASL CN2
- di dare mandato a tutti gli autorizzati al trattamento dati, dipendenti e non, di prendere visione della procedura e di osservare le indicazioni ivi contenute, ricordando che una violazione di dati personali può – se non affrontata in modo adeguato e tempestivo – provocare danni fisici, materiali o immateriali alle persone fisiche;
- di dare atto che il responsabile del procedimento è la Dott.ssa Tiziana ROSSINI, Responsabile f.f. S.S. Affari Generali e Segreteria Organismi Collegiali, nonché Coordinatore del Gruppo Privacy Aziendale;
- di dare atto che il presente provvedimento non comporta oneri di spesa;
- di demandare alla S.S. Affari Generali e Segreteria Organismi Collegiali l'invio del presente atto ai seguenti destinatari:
 - tutti gli autorizzati privacy;

- DPO – Avv. Giuseppe CANNELLA privacyaslcn2@lexlecis.com

- di dichiarare la presente deliberazione, vista l'urgenza di provvedere in merito, immediatamente esecutiva, ai sensi dell'art. 3, comma 2 della Legge Regionale 30 giugno 1992, n. 31 e s.m.i.;

Letto, approvato e sottoscritto.

IL DIRETTORE GENERALE
Paola MALVASIO

Sottoscrizione per conferma del parere richiamato nel contesto della determinazione:

IL DIRETTORE SANITARIO
Luca BURRONI

IL DIRETTORE AMMINISTRATIVO
Claudio MONTI

Sottoscrizione per proposta:

IL RESPONSABILE FF SS AFFARI GENERALI E
SEGRETERIA ORGANISMI COLLEGIALI
Tiziana ROSSINI

Documento informatico firmato digitalmente ai sensi di legge

Archivio: I.1.10 Fascicolo Proc.

Allegati. A) Procedura Data Breach "PSinteraziendale003-Revisione n.01"

Avverso i provvedimenti dell'ASL l'interessato può proporre:

RICORSO AL T.A.R.

Tale ricorso è finalizzato alla tutela di diritti soggettivi ed interessi legittimi.

Tale ricorso deve essere presentato

- *nel termine perentorio di 30 gg. nel caso di appalti, con decorrenza dalla data della pubblicazione del provvedimento sul sito ASL CN2 (ex art. 204 del D.lg.vo 50/2016)*
- *nel termine perentorio di 60 gg. in tutti gli altri casi, con decorrenza dalla data in cui l'interessato ha ricevuto la notifica del provvedimento o ne ha avuto pieno conoscenza*

RICORSO STRAORDINARIO AL PRESIDENTE DELLA REPUBBLICA

Tale ricorso, alternativo al ricorso avanti al T.A.R., è anch'esso finalizzato alla tutela di diritti soggettivi ed interessi legittimi.

Esso non è ammesso per i provvedimenti di affidamento di appalti.

Tale ricorso deve essere presentato nel termine di 120 gg. decorrenti dalla data in cui l'interessato ha ricevuto la notifica del provvedimento o ne ha avuto pieno conoscenza.

RICORSO AL GIUDICE ORDINARIO

Tale ricorso è finalizzato alla tutela di un diritto soggettivo.

Tale ricorso deve essere presentato nel termine di prescrizione dell'azione previsto dal Codice Civile.