Sistema Socio Sanitario
Ospedale Maggiore
Regione Lombardia
ASST Crema

VERBALE DI DELIBERAZIONE N. 782

UOC Affari Generali e Legali

Il Responsabile del procedimento: Elena Nolli

VERBALE DI DELIBERAZIONE DEL DIRETTORE GENERALE

Il giorno 29/12/2021 presso la sede legale, il Direttore Generale nella persona del Dott. Ida Maria Ada Ramponi ha adottato la seguente deliberazione.

OGGETTO: **APPROVAZIONE DELLA PROCEDURA OPERATIVA PER LA GESTIONE DELLA VIOLAZIONE DEI DATI PERSONALI - DATA BREACH**

ASSISTITO DA:

IL DIRETTORE AMMINISTRATIVO	Dott. Maurizia Ficarelli
IL DIRETTORE SANITARIO	Dott. Roberto Sfogliarini
IL DIRETTORE SOCIOSANITARIO	Dott. Diego Maltagliati

IL DIRETTORE GENERALE

Richiamate:

La LR 30.12. 2009 n. 33 “Testo unico delle leggi regionali in materia di sanità”;

La DGR n. X/4496 del 10.12.2015 con la quale è stata disposta la costituzione dell’Azienda Socio Sanitaria Territoriale (ASST) di Crema;

La DGR n. XI/5204 del 7.09.2021 di nomina della dott.ssa Ida Maria Ada Ramponi quale Direttore Generale della ASST di Crema;

Rilevato che il Responsabile del procedimento riferisce quanto segue:

RICHIAMATO il Regolamento (UE) 2016/679 sulla protezione dei dati – General Data Protection Regulation (GDPR) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali;

RICHIAMATA la deliberazione n. 520 del 23.12.2019 con cui si è proceduto ad approvare apposita regolamentazione per l’attuazione in ambito aziendale del Regolamento UE 2016/679;

RICORDATO che il citato provvedimento tratta in apposito paragrafo la gestione del “data breach” ovvero della violazione dei dati personali, intendendosi la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l’accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati dall’Azienda;

RILEVATO che, secondo la disciplina aziendale sopracitata:

a) il Titolare del trattamento, ove ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati, provvede alla notifica della violazione al Garante Privacy, entro 72 ore e comunque senza ingiustificato ritardo;

b) qualora il Titolare ritenga che il rischio per i diritti e le libertà degli interessati conseguente alla violazione rilevata sia elevato, deve informare questi ultimi, senza ingiustificato ritardo, al fine di fare comprendere loro la natura della violazione dei dati personali verificatesi. I rischi per i diritti e le libertà degli interessati possono essere considerati “elevati” quando la violazione può, a titolo di esempio:

- coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;

- riguardare categorie particolari di dati personali;

- comprendere dati che possono accrescere ulteriormente i potenziali rischi;

- comportare rischi imminenti e con un’elevata probabilità di accadimento;

- impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni;

c) il Titolare deve opportunamente documentare le violazioni di dati personali subite, anche se non comunicate all’Autorità di controllo, nonché le circostanze ad esse relative, le conseguenze e i provvedimenti adottati o che intende adottare per porvi rimedio;

VISTI, in particolare, gli artt. 33 e 34 del GDPR disciplinanti le modalità di notifica all’Autorità di controllo e di comunicazione all’interessato/i delle violazioni dei dati personali;

RICHIAMATA altresì la deliberazione n. 380 del 2.07.2021 con cui si è proceduto a formalizzare, ex art. 37 del Regolamento UE 2016/679, la nomina, in qualità di Data Protection Officer (DPO) della ASST di Crema, della società LTA Srl di Roma, sino al 27.06.2023;

VALUTATO opportuno approntare una procedura aziendale recante istruzioni operative per la gestione dei casi di violazione dei dati personali nonché degli adempimenti di comunicazione conseguenti (all’Autorità di controllo ed ai soggetti interessati);

VISTO il testo della “Procedura per la gestione delle violazioni di dati personali” predisposta dall’UOC Affari Generali e Legali con il supporto del DPO, il cui testo è allegato al presente atto quale parte integrante;

RISCONTRATO, in particolare, che la gestione del "data breach" verrà effettuata con utilizzo dell'applicativo MUA fornito dal DPO aziendale tramite il quale verranno generati appositi flussi per effetto dell'inserimento delle informazioni richieste (cfr. documento "Descrizione flusso data breach" allegato alla procedura operativa, in cui sono dettagliamente descritte le fasi operative della procedura di gestione delle violazioni);

RITENUTO di approvare la "Procedura per la gestione delle violazioni di dati personali" nonché il relativo allegato denominato "Descrizione flusso data breach", nella versione acclusa al presente provvedimento;

RITENUTO altresì di individuare il Dirigente Responsabile della UOC Affari Generali e Legali quale "Responsabile della gestione del data breach";

DATO ATTO che il presente provvedimento viene adottato su proposta del Dirigente dell'UO Affari Generali e Legali che ne attesta la regolarità tecnica e la legittimità del provvedimento;

DATO ATTO che dall'adozione del presente provvedimento non derivano oneri a carico del bilancio aziendale;

ACQUISITO il parere del Direttore Amministrativo, Direttore Sanitario e del Direttore Socio Sanitario per quanto di competenza così come previsto dall'art. 3 del Decreto Legislativo 30.12.1992 n. 502 e successive modificazioni;

DELIBERA

di prendere atto di quanto in premessa descritto e conseguentemente:

1)di approvare la "Procedura per la gestione delle violazioni di dati personali" nonché il relativo allegato denominato "Descrizione flusso data breach", nella versione acclusa al presente provvedimento;

2)di individuare il Dirigente Responsabile della UOC Affari Generali e Legali quale "Responsabile della gestione del data breach";

3)di riservarsi di disporre, con ulteriori provvedimenti, una nuova approvazione della procedura operativa in oggetto conseguente a successivi aggiornamenti della medesima;

4)di dare atto che dall'adozione del presente provvedimento non derivano oneri a carico del bilancio aziendale.

Parere favorevole:

IL DIRETTORE AMMINISTRATIVO — F.to Dott. Maurizia Ficarelli

IL DIRETTORE SANITARIO — F.to Dott. Roberto Sfogliarini

IL DIRETTORE SOCIOSANITARIO — F.to Dott. Diego Maltagliati

IL DIRETTORE GENERALE

F.to Dott. Ida Maria Ada Ramponi

Ai fini della pubblicazione la firma autografa è sostituita con indicazione a stampa del nominativo del soggetto responsabile ai sensi del D.L.vo n. 39/1993, art. 3, comma 2

PROCEDURA DI GESTIONE DELLE VIOLAZIONI DI DATI PERSONALI (DATA BREACH)

1. *Scopo*

La presente procedura ha lo scopo di gestire il necessario flusso di attività da porre in essere nel momento in cui si sviluppi una violazione di dati personali ai sensi degli articoli 33 e 34 del Regolamento 679/2016/UE.

Per "data breach" (violazione dei dati personali), si intende una violazione di sicurezza che comporta accidentalmente o illecitamente la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Il Regolamento Europeo 679/2016/UE prevede che, in caso di violazione dei dati personali, il Titolare del trattamento debba notificare 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.

La procedura sarà gestita tramite il flusso "data breach" presente in MUA–Motore Unico Amministrativo tramite la compilazione di un questionario on-line e coinvolgerà le diverse unità organizzative che segnaleranno l'avvenuta violazione, la UOC Affari Generali e Legali (AGL) quale funzione aziendale competente in materia di protezione dei dati ed il Data Protection Officer (DPO).

2. *Casi nei quali avviare la procedura di gestione della violazione dei dati personali (data breach)*

I casi in cui sarà necessario applicare la presente procedura sono, a titolo esemplificativo e non esaustivo, i seguenti:

- Sottrazione di credenziali di autenticazione
- Furto di PC, Notebook, Tablet, Smartphone contenente dati personali
- Erronea diffusione, pubblicazione, comunicazione di dati personali
- Intrusione non autorizzata in locali in cui sono conservati/archiviati dati personali
- Furto di archivi cartacei e/o digitali
- Accesso non autorizzato nel sistema informativo
- Azione di malware (virus, etc.) che siano riusciti ad eludere le misure di sicurezza aziendali
- Smarrimento di dati personali (archiviati su supporti cartacei e digitali)

- Distruzione di dati personali (archiviati su supporti cartacei e digitali)

3. *Procedura di gestione della violazione dei dati personali (data breach)*

Nel caso in cui un soggetto venga a conoscenza di una concreta, potenziale o sospetta violazione di dati personali, dovrà essere attivato il flusso di adempimenti di seguito descritti e schematizzati.

La gestione della violazione concreta, potenziale o sospetta prevede l'attuazione delle seguenti attività:

A. rilevazione della violazione dei dati personali
B. raccolta di informazioni sulla violazione
C. comunicazione della violazione al Responsabile della UOC Affari Generali e Legali (Responsabile AGL) che procederà ad una prima analisi della violazione di concerto con il Direttore Generale quale Titolare del trattamento e con il DPO.
D. compilazione della prima parte del flusso di data breach fino a chiusura della sezione (step A-B-C)
E. compilazione da parte del Responsabile AGL, con il supporto del DPO, della seconda parte del Flusso e valutazione della necessità di effettuare la comunicazione all'Autorità Garante
F. notifica all'Autorità Garante della violazione subita, nel caso in cui la violazione comporti un rischio per i diritti e la libertà delle persone fisiche
G. eventuale comunicazione della violazione di dati personali all'interessato nel caso vi sia un rischio elevato (il documento per la segnalazione agli interessati potrà essere generato tramite il flusso dei "data breach")
H. nel caso in cui si sia valutato di non effettuare comunicazione all'Autorità Garante, sarà necessario registrare la violazione all'interno del sistema MUA tramite lo svolgimento del Flusso di segnalazione di data breach, al fine di mantenere aggiornato il "Registro degli incidenti". Tale registro sarà reperibile all'interno del sistema nella pagina "Elementi di analisi", alla voce "Regolamento 679/2016/UE - Data breach"

4. *Soggetti deputati ad avviare la procedura di gestione della violazione*

A seguito della rilevazione della violazione di dati personali, la procedura di gestione della violazione verrà avviata, tramite il sistema MUA, dal Responsabile AGL.

Ai fini dell'avvio della procedura di gestione della violazione di dati personali, il Responsabile AGL coinvolgerà :

1. il referente (interno o esterno) del servizio che ha subito la violazione;
2. il Responsabile dei Sistemi Informativi Aziendali qualora la violazione riguardi un asset tecnologico-informatico, al fine di valutare la portata della violazione e descrivere dettagliatamente l'accaduto.

5. *Modalità di avvio della procedura di gestione della violazione*

L'avvio della procedura di gestione data breach dovrà essere sviluppata seguendo le seguenti fasi:

1. comunicazione/segnalazione dell'evento che può comportare una violazione di dati al Responsabile della UOC Affari Generali e Legali;
2. il soggetto incaricato dal Responsabile UOC Affari Generali e Legali nell'ambito della propria U.O. deve raccogliere, prima dell'avvio del flusso, tutte le informazioni necessarie;
3. l'incaricato procede con l'accesso nominativo al sistema MUA attraverso l'indirizzo web https://mua.secoges.com e avvia il flusso "Privacy – Data breach" secondo le istruzioni descritte nell'allegato 1 "Descrizione del flusso data breach";
4. l'incaricato deve rispondere alle domande del questionario presenti in MUA relative a:
- identificazione e descrizione dell'evento
- misure tecnologiche e organizzative applicate alla protezione dei dati (prima, durante e dopo la violazione)
- informazioni relative ai soggetti individuati per la gestione della procedura; se necessario dovrà farsi affiancare nella sua compilazione da coloro che sono in possesso delle informazioni

5. conclusa la compilazione del questionario l'incaricato chiude il flusso
6. a questo punto il flusso incarica il Responsabile AGL dello svolgimento della seconda parte del medesimo;
7. il Responsabile AGL riceve una mail dal sistema MUA che lo informa che è stato incaricato di svolgere la seconda parte del flusso
8. il Responsabile AGL accede al sistema MUA attraverso l'indirizzo web https://mua.secoges.com dove trova evidenziato in rosso il pulsante "Attività da svolgere" e attiva il flusso attivo chiamato "Privacy – Data breach"
9. il Responsabile AGL visualizza all'interno del sistema MUA le informazioni inserite durante la prima parte del flusso;
10. in base alle informazioni inserite il Responsabile AGL valuta, di concerto con il DPO, la necessità di fare comunicazione all'Autorità Garante e agli interessati e procede con la compilazione del questionario;

11. il Responsabile AGL procede fino alla chiusura del flusso in MUA:

11.1. *Caso A:* incidente da inserire nel registro incidenti

11.1.1. inserimento della violazione nel registro incidenti

11.1.2. comunicazione da parte del DPO di chiusura dell'incidente

11.2 *Caso B (*incidente da inserire nel registro incidenti e da notificare all'Autorità Garante (nel caso in cui la violazione comporti un rischio per i diritti e la libertà delle persone fisiche)

11.2.1 inserimento della violazione nel registro incidenti

11.2.2 generazione del modulo (*fac-simile*) di comunicazione di Data Breach

11.2.3 trasmissione della comunicazione di chiusura della procedura da parte del Responsabile AGL alla mail indicata durante lo svolgimento del flusso

11.2.4 acquisizione, mediante download, del modulo (*fac-simile*) di comunicazione all'Autorità Garante nel seguente modo:

- accedere alla sezione "Elementi d'analisi" alla voce "Regolamento 679/2016/UE - Data breach"
- posizionarsi sulla violazione/incidente inserito
- espandere la sezione "File allegati"
- cliccare sul documento da scaricare denominato "Modello di comunicazione al Garante-Data breach"
- la documentazione viene inviata anche mezzo mail agli indirizzi indicati durante lo svolgimento del flusso

11.2.5 utilizzo del modulo (*fac-simile*) di comunicazione di Data Breach quale bozza di riferimento per la notifica della violazione dei dati personali all'Autorità Garante

11.2.6 notifica della violazione dei dati personali secondo le modalità operative previste dall'Autorità Garante e rese accessibili sul sito dell'Autorità

11.2.7 trasmissione al DPO – per conoscenza – del modulo di notifica della violazione dei dati personali effettuata sul sito ufficiale dell'Autorità

11.2.8 acquisizione in MUA del modulo di notifica della violazione dei dati personali nel seguente modo:

- accedere alla sezione "Elementi d'analisi" alla voce "Regolamento 679/2016/UE - Data breach"
- posizionarsi sulla violazione/incidente inserito
- espandere la sezione "File allegati"
- cliccare su "Nuovo" e successivamente su "Seleziona il file da allegare"
- caricare il modulo di notifica della violazione dei dati personali e cliccare su "salva allegati"

11.3 *Caso C* (incidente da inserire nel registro incidenti, da notificare all'Autorità Garante e da comunicare agli interessati (nel caso in cui la

violazione comporti un rischio elevato per i diritti e la libertà delle persone fisiche)

11.3.1 inserimento della violazione nel registro degli incidenti e invio notifica all'Autorità Garante come da punti da 11.2.1 a 11.2.8

11.3.2 comunicazione della violazione di dati personali all'interessato

ALLEGATO 1:

Descrizione del flusso data breach.

DESCRIZIONE FLUSSO DATA BREACH

Modalità di avvio del flusso di gestione delle violazioni (data breach)

Avvio del flusso di gestione del data breach:

1. l'incaricato allo svolgimento del flusso dovrà raccogliere, prima dell'avvio del flusso, le informazioni che verranno richieste all'interno di quest'ultimo, oppure farsi affiancare nella sua compilazione da coloro che sono in possesso di queste informazioni
2. l'incaricato accederà al sistema MUA attraverso l'indirizzo web https://mua.secoges.com
3. l'incaricato inserirà le proprie credenziali di autenticazione
4. l'incaricato cliccherà il pulsante all'interno della home page denominato "Workflow per ambito normativo"
5. l'incaricato cliccherà sul simbolo "+" accanto alla dicitura "Pacchetto GDPR"
6. l'incaricato cliccherà sulla dicitura "Privacy – Data breach"
7. l'incaricato risponderà alle domande del questionario

Descrizione del flusso del data breach

Step A. Identificazione e descrizione dell'evento:

Indicare la tipologia di comunicazione che si sta facendo all'Autorità Garante; il flusso chiederà che tipo di notifica si sta effettuando:

- Preliminare (il Titolare del trattamento avvia una procedura di segnalazione senza avere un quadro completo della violazione e si riserva di effettuare una successiva notifica integrativa)
- Completa
- Integrativa (il Titolare del trattamento integra una precedente notifica). Nel caso di notifica integrativa il flusso permetterà di importare le informazioni della preliminare. Se si sta facendo una segnalazione integrativa il flusso richiederà, se noto, il numero di fascicolo assegnato alla precedente notifica dall'Autorità Garante

Selezionare gli strumenti hardware, software o locali fisici oggetto della violazione/incidente (se il sistema non è ancora stato popolato con queste informazioni, il flusso permetterà di inserire l'elemento che ha subìto la violazione). Se associati, il sistema permetterà di indicare quali trattamenti collegati all'elemento violato sono stati oggetto della violazione.

Nel caso in cui i collegamenti non siano stati ancora effettuati, il flusso dà la possibilità di indicare quali trattamenti sono stati oggetto di violazione.

Descrivere l'evento che ha condotto alla violazione subìta

Indicare quando è avvenuta la violazione

Indicare la data e l'ora in cui il Titolare del trattamento è venuto a conoscenza della violazione

Indicare le modalità con le quali il Titolare è venuto a conoscenza della violazione (per il tramite del responsabile del trattamento o in altro modo)

Indicare se nel trattamento sono coinvolti ulteriori soggetti esterni. Il flusso permette di scegliere un soggetto tra quelli presenti in elenco "Enti Esterni" oppure di inserire un nuovo soggetto.

Le informazioni che dovranno essere inserite sono:

- Denominazione (indicare il nome e cognome in caso di persona fisica)
- Codice fiscale/Partita Iva
- Ruolo: Co-titolare, Responsabile esterno ai sensi dell'Art. 28

Indicare le possibili cause della violazione. Scegliere fra le possibilità presenti:

- Azione intenzionale interna
- Azione accidentale interna
- Azione intenzionale eterna
- Azione accidentale esterna
- Sconosciuta
- Altro

Scegliendo "Altro" il flusso permette di indicare altre possibili cause della violazione.

Indicare la natura della violazione scegliendo una o più delle seguenti risposte:

- Perdita di confidenzialità (diffusione/accesso non autorizzato o accidentale);
- Perdita di integrità (modifica non autorizzata o accidentale);
- Perdita di disponibilità (impossibilità di accesso, perdita, distruzione non autorizzata o accidentale).

Per ognuna delle risposte selezionate il flusso chiede di specificare ulteriormente la natura della violazione e indicare le possibili conseguenze della violazione sugli interessati (è possibile selezionare più di una risposta).

Indicare il volume dei dati violati (ad esempio il numero di referti, numero di record di un database, numero di transazioni registrate). Se il numero non è conosciuto, selezionare la voce "Un numero (ancora) non definito di dati".

Indicare il numero di interessati coinvolti nella violazione.

Se il numero non è conosciuto selezionare la voce "Un numero (ancora) sconosciuto di interessati".

Indicare le possibili categorie di interessati coinvolte nella violazione.

Nel caso in cui precedentemente siano stati individuati i trattamenti oggetto della violazione, il sistema riproporrà le relative categorie di interessati.

Nel caso in cui non siano stati selezionati i trattamenti, sarà necessario indicare le possibili categorie d'interessati, scegliendo dal menù in elenco (è possibile selezionare più di una risposta).

Step B: Misure tecnologiche e organizzative applicate a protezione dei dati (prima, durante e dopo la violazione)

Indicare le misure tecnologiche e organizzative adottate per garantire la sicurezza dei dati, dei sistemi e delle infrastrutture IT coinvolti nella violazione.

Indicare le misure tecniche e organizzative adottate (o di cui si propone l'adozione futura) per porre rimedio alla violazione e ridurne gli effetti negativi per gli interessati.

Nella descrizione distinguere fra le misure già adottate e quelle in corso di adozione.

Indicare le misure tecniche e organizzative adottate (o di cui si propone l'adozione futura) per prevenire simili violazioni future.

Step C. Ulteriori informazioni

Indicare il nominativo del soggetto deputato alla notifica al Garante (scegliere nel menù in elenco). Nel caso in cui queste informazioni non siano presenti nel sistema verranno richieste:

- Cognome e nome del segnalante
- E-mail
- Recapito telefonico per eventuali comunicazioni
- Funziona rivestita

Dati relativi al Titolare del trattamento

- Denominazione
- Codice fiscale/Partita Iva
- Stato
- Indirizzo
- CAP
- Città
- Provincia
- E-mail

- Pec

Il flusso incarica il Responsabile AGL dello svolgimento della seconda parte del medesimo. Il Responsabile AGL riceverà una comunicazione tramite mail dell'avvenuto incarico.

Step D. Comunicazione della violazione

In base alle informazioni inserite, il Responsabile AGL valuta, di concerto con il DPO, la necessità di fare comunicazione all'Autorità Garante. Qualora si voglia notificare la violazione al Garante, il sistema genera il documento sulla base del modello predisposto dall'Autorità Garante.

In ogni caso, il sistema registra tutte le informazioni al fine di implementare il registro delle violazioni

↓

Indicare se la comunicazione è effettuata ai sensi:

- Dell'Art.33 GDPR
- Dell'Art. 26 D.lgs 51/2018

↓

Indicare i riferimenti del soggetto da contattare per ottenere maggiori informazioni circa la violazione.

Nel caso in cui sia stato individuato il DPO, indicare il numero di protocollo assegnato alla comunicazione all'Autorità Garante dei dati di contatto del DPO.

In alternativa, indicare il soggetto da contattare:

- Cognome e Nome
- E-mail
- Recapito telefonico per eventuali comunicazioni
- Funzione rivestita

↓

Nel caso in cui la comunicazione venga effettuata oltre le 72 ore, il flusso chiederà di motivare il ritardo.

↓

Descrivere l'incidente alla base della violazione.

↓

Descrivere le categorie di dati personali oggetto della violazione.

↓

Indicare tipologie di dati coinvolti nella violazione.
Se durante la prima parte del flusso sono stati selezionati dei trattamenti, il flusso leggerà e preselezionerà le tipologie di dati già indicate sul trattamento.

Indicare, per ogni tipo di dato scelto o collegato ai trattamenti coinvolti nella violazione, le specifiche categorie di dati.

Indicare la stima della violazione.

Indicare le motivazioni della scelta.

Step E. Comunicazione agli interessati

Indicare i potenziali effetti negativi della violazione sugli interessati.

- Se tra le voci si seleziona "Nessun rischio", il flusso indicherà che non vi è necessità di fare comunicazione agli interessati.
- Se si seleziona uno dei rischi in elenco, il flusso chiederà di indicare se ci sono delle motivazioni per cui non deve essere fatta comunicazione agli interessati (fattispecie esimenti ai sensi dell'art. 34, par. 4, GDPR):
  - se ricorre una delle fattispecie esimenti, il flusso indicherà che non deve essere fatta comunicazione agli interessati;
  - se nessuna delle fattispecie esimenti è applicabile al caso di specie, il flusso indicherà che deve essere fatta comunicazione agli interessati.

Nel caso in cui si sia presa la decisione di effettuare la comunicazione agli interessati, inserire il testo della comunicazione che si intende dare agli interessati.

Nel caso in cui si sia presa la decisione di effettuare la comunicazione agli interessati, indicare la modalità con cui è stata data o si darà loro comunicazione.

Nel caso in cui si sia presa la decisione di effettuare la comunicazione agli interessati, il flusso genererà il documento da inviare agli stessi.

Nel caso in cui si sia presa la decisione di fare comunicazione all'Autorità Garante, verrà generato il modulo (*fac-simile*) di comunicazione di data breach.

Il flusso invierà la documentazione generata agli indirizzi mail dichiarati. La documentazione generata sarà scaricabile accedendo alla sezione "Elementi d'analisi" alla voce "Regolamento 679/2016/UE - Data breach". Selezionare l'evento per cui si intende scaricare la documentazione (che sarà presente nella sezione "File allegati").

Nel caso in cui sia stato valutato di non effettuare la notifica all'Autorità Garante, verrà comunque inviata notifica della conclusione del flusso e della decisione di non fare comunicazione all'Autorità Garante.

Indicare gli indirizzi e-mail a cui sarà inviata l'eventuale documentazione generata dal flusso e la

comunicazione di conclusione del flusso.

Step F. Chiusura dell'incidente

Descrivere il modo di risoluzione della violazione/incidente, nel caso sia stato risolto. Indicare la data di risoluzione della violazione/incidente, nel caso sia stato risolto.

Deliberazione di UOC Affari Generali e Legali

OGGETTO: APPROVAZIONE DELLA PROCEDURA OPERATIVA PER LA GESTIONE DELLA VIOLAZIONE DEI DATI PERSONALI - DATA BREACH

ATTESTAZIONE DI REGOLARITA' TECNICA

Il Responsabile del Procedimento attesta la regolarità tecnica e la leggitimità della proposta sopra citata.

Il Direttore di UOC Affari Generali e Legali

(F.to Dott. Elena Nolli)

.....

Ai fini della pubblicazione la firma autografa è sostituita con indicazione a stampa del nominativo del soggetto responsabile ai sensi del D.L.vo n. 39/1993, art. 3, comma 2

Data, 24/12/2021

ATTESTAZIONE DI REGOLARITA' CONTABILE

Il Responsabile dell'ufficio UOC Programmazione Bilancio e Contabilità attesta la copertura economica e la regolarità contabile della proposta della deliberazione sopra riportata.

Il Responsabile di UOC Programmazione Bilancio e Contabilità

(F.to Dott. Marco Brusati)

.....

Ai fini della pubblicazione la firma autografa è sostituita con indicazione a stampa del nominativo del soggetto responsabile ai sensi del D.L.vo n. 39/1993, art. 3, comma 2

Data, 27/12/2021