LIBERO CONSORZIO COMUNALE DI RAGUSA

Deliberazione del Commissario Straordinario

con i poteri della Giunta Provinciale ex art. 51 L.R. 15/2015

Registro Staff Segreteria Generale n. 34/2021	Deliberazione n. 34 /2021
OGGETTO: Adozione del documento di definizione della "Procedura per la gestione degli incidenti informatici e delle violazioni dei dati personali (data breach)"	

L'anno 2021, il giorno VENTINOVE **del mese di** MARZO **alle ore** 10.45 **in Ragusa, presso il Palazzo del Libero Consorzio Comunale, il Commissario Straordinario, Dott. Salvatore Piazza, nominato con Decreto del Presidenza della Regione Siciliana n.517/GAB dell'1/02/2021, ed assunti i poteri e le funzioni della Giunta, assistito dal Segretario Generale Dott Alberto D'Arrigo**

PROPOSTA DI DELIBERAZIONE

Staff Segreteria Generale

Il Segretario Generale

Premesso che

- il regolamento (UE) n. 679/2016 del Parlamento Europeo e del Consiglio del 27 aprile 2016, più comunemente chiamato G.D.P.R.(General Data Protection Regulation), stabilisce le nuove norme in materia di protezione delle persone fisiche, con riguardo al trattamento dei dati personali, nonchè alle norme relative alla libera circolazione dei dati;
- detto regolamento prevede il principio di "accountability" (obbligo di responsabilizzazione) che impone al titolare del trattamento di mettere in atto tutte le misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, tenendo conto dello stato dell'organizzazione dell'Ente e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento;

- il Libero Consorzio Comunale di Ragusa, nell'ambito delle proprie attività, raccoglie e tratta dati personali per le proprie finalità istituzionali e per le proprie esigenze organizzative, agendo in qualità di "titolare del trattamento".
- rientra tra i doveri del titolare la regolamentazione della gestione delle violazioni dei dati personali – i cosiddetti *data breach* – che possono incorrere ai dati personali conservati e trattati dallo stesso. La corretta gestione degli incidenti di sicurezza, infatti, permette di evitare o minimizzare la compromissione dei dati di questo Ente in caso di incidente, tutelando altresì i diritti e le libertà fondamentali dei soggetti interessati dalle attività di trattamento dei dati personali effettuate dalla stessa in qualità di titolare del trattamento; permette inoltre, attraverso l'analisi e la comprensione dei meccanismi di attacco e delle modalità utilizzate per la gestione dell'incidente, di migliorare continuamente la capacità di risposta agli incidenti
- l'art. 32 del GDPR stabilisce, infatti, che devono essere approntate misure tecniche e organizzative atte a garantire un livello adeguato di sicurezza dei dati personali. Individuare, indirizzare e segnalare tempestivamente un incidente di sicurezza, specie se lo stesso comporta una violazione di dati personali, è espressione dell'adeguatezza delle misure implementate da questo Ente e quindi del rispetto del principio di *accountability* in capo alla stessa nella sua qualità di titolare del trattamento, ai sensi dell'art. 5, par. 2, del Regolamento UE 2016/679.

Considerato che occorre procedere a sopraddetta regolamentazione che definisca delle precise istruzioni operative, da applicare ai soggetti che trattano dati personali per conto di questo Ente, nella sua qualità di titolare del trattamento.

Visto il documento, allegato alla presente deliberazione, che:

- con riferimento all'art 33 del G.D.P.R. riporta una apposita procedura finalizzata ad individuare quali siano le violazioni che ricadono nell'ambito della suddetta normativa, nonché i casi in cui il Libero Consorzio Comunale di Ragusa deve notificare le violazioni dei dati personali *(data breach)* all'Autorità Garante per la protezione dei dati personali ed eventualmente agli interessati ai sensi dell'art. 34 del GDPR;
- definisce le misure atte a trattare e minimizzare i rischi per i diritti e le libertà delle persone interessate dallo specifico trattamento, nonché la documentazione da produrre in aderenza a quanto prescritto dalla normativa vigente in materia di protezione dei dati personali.
- definisce delle precise istruzioni operative, da applicare ai soggetti che trattano dati personali per conto del Libero Consorzio Comunale di Ragusa, nella sua qualità di titolare del trattamento. L'ambito di applicazione è rappresentato da tutti i sistemi e gli archivi informativi del LCC– sia che trattino dati in formato cartaceo, che automatizzato – e vengono presi in considerazione incidenti che possono scaturire sia attraverso l'azione di un attacco portato da elementi esterni a questo Ente e, sia generati da un eventuale comportamento scorretto di un dipendente o di un collaboratore dello stesso.

Ritenuto, pertanto, di approvare la procedura per la gestione degli incidenti informatici e delle violazioni dei dati personali (data breach) di cui all'allegato documento che fa parte integrale e sostanziale della presente deliberazione.

Visti:
-il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016;
-il Decreto Legislativo n. 196 del 30 giugno 2003 recante il *"Codice in materia di protezione dei dati personali"* integrato con le modifiche introdotte dal Decreto Legislativo n. 101 del 10 agosto 2018.

In relazione a quanto sopra esposto,

PROPONE

1. di approvare il documento "Procedura per la gestione degli incidenti informatici e delle violazioni dei dati personali (data breach)", ai sensi degli artt 33 e 34 del G.D.P.R.(General Data Protection Regulation) ed il modello per la comunicazione della violazione dei dati personali, allegati alla presente deliberazione e che ne costituiscono parte integrante e sostanziale;

2. di dare atto che le disposizioni operative sono assoggettate a revisione ogni qualvolta si renderà necessario e, comunque, a cadenza almeno annuale.

3. di demandare la concreta attuazione delle misure regolamentari sopraddette, al personale di questo Ente, nelle sue articolazioni gerarchiche e secondo le rispettive funzioni e competenze, detto personale, ove richiesto, dovrà fornire pieno supporto al titolare del trattamento ed al responsabile per la protezione dei dati nell'esecuzione delle attività descritte dalla procedura in questione;

4. di disporre che al presente provvedimento venga assicurata la pubblicità legale mediante pubblicazione all'Albo Pretorio dell'Ente, nonché la massima diffusione presso i soggetti autorizzati, anche tramite pubblicazione sulla rete intranet dell'Ente;

5. di dare atto della mancanza del conflitto di interesse, anche potenziale, in capo al sottoscritto proponente, in ordine al presente procedimento;

6. di dare atto che il presente provvedimento è soggetto alla pubblicazione per estratto ai sensi della L.R. n. 22/2008;

7. Di dare atto che dall'adozione della presente deliberazione non derivano oneri aggiuntivi a carico del bilancio di questo Ente.

IL SEGRETARIO GENERALE
Dott Alberto D'Arrigo

Attestazione di regolarità procedimentale - Ai sensi ed agli effetti dell'art.7 della L.R. 21/05/2019, n.7, attesta che nella formazione della proposta di deliberazione di cui sopra sono state valutate le condizioni di ammissibilità, i requisiti di legittimità e i presupposti ritenuti

Registro di Settore n. 31 /2021	Deliberazione n. 34	29 MAR 2021

rilevanti per l'assunzione del provvedimento ed è stata eseguita la procedura prescritta dalla vigente normativa di legge e regolamentare in materia.

Ragusa 29.03.2021

IL RESPONSABILE DEL PROCEDIMENTO
(Mariarosaria Schembari)
Mariarosaria Schembari

Parere di regolarità tecnica - Ai sensi e per gli effetti dell'art.53 della Legge 08.06.1990, n.142, richiamato dall'art.1, comma primo, lett. i), della L.R. 11.12.1991, n.48, modificato da ultimo dall'art.12 della L.R. 23.12.2000, n.30, in ordine alla regolarità tecnica del presente provvedimento si esprime il seguente parere: favorevole

Ragusa 29.03.2021

IL SEGRETARIO GENERALE
(Dott Alberto D'Arrigo)

SETTORE CONTABILITA' E BILANCIO

Parere di regolarita' contabile - Ai sensi e per gli effetti dell'art.53 della Legge 08.06.1990 n.142, richiamato dall'art.1, comma 1°, lett. i) della L.R. 11.12.1991, n. 48, modificato dall'art.12 della L.R. 23.12.2000, n.30,e dell'art..49, primo comma, del D. Leg.vo 18.08.2000, n.267, in ordine alla regolarità contabile del presente provvedimento si esprime il seguente parere: favorevole .....

Ragusa, 29.03.2021

IL DIRIGENTE
Dott Giuseppe Digiorgio

IL COMMISSARIO STRAORDINARIO

VISTA la suesposta proposta di deliberazione contenente le motivazioni che giustificano l'adozione del presente provvedimento;

RICHIAMATA integralmente la parte motiva della proposta de qua;

VISTO il parere di regolarità tecnica in ordine al presente provvedimento, rilasciato dal Segretario Generale responsabile del servizio;

VISTI:
-il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016;
-il Decreto Legislativo n. 196 del 30 giugno 2003 recante il *"Codice in materia di protezione dei dati personali"* integrato con le modifiche introdotte dal Decreto Legislativo n. 101 del 10 agosto 2018.

DELIBERA

1. di approvare il documento "Procedura per la gestione degli incidenti informatici e delle violazioni dei dati personali (data breach)", ai sensi degli artt 33 e 34 del G.D.P.R.(General Data Protection Regulation) ed il modello per la comunicazione della violazione dei dati personali, allegati alla presente deliberazione e che ne costituiscono parte integrante e sostanziale;

2. di dare atto che le disposizioni operative sono assoggettate a revisione ogni qualvolta si renderà necessario e, comunque, a cadenza almeno annuale.

Registro di Settore n. 31 /2021	Deliberazione n. 31	29 MAR 2021

3. di demandare la concreta attuazione delle misure regolamentari sopraddette, al personale di questo Ente, nelle sue articolazioni gerarchiche e secondo le rispettive funzioni e competenze, detto personale, ove richiesto, dovrà fornire pieno supporto al titolare del trattamento ed al responsabile per la protezione dei dati nell'esecuzione delle attività descritte dalla procedura in questione;

4. di disporre che al presente provvedimento venga assicurata la pubblicità legale mediante pubblicazione all'Albo Pretorio dell'Ente, nonché la massima diffusione presso i soggetti autorizzati, anche tramite pubblicazione sulla rete intranet dell'Ente;

5. di dare atto della mancanza del conflitto di interesse, anche potenziale, in capo al sottoscritto proponente, in ordine al presente procedimento;

6. di dare atto che il presente provvedimento è soggetto alla pubblicazione per estratto ai sensi della L.R. n. 22/2008;

7. Di dare atto che dall'adozione della presente deliberazione non derivano oneri aggiuntivi a carico del bilancio di questo Ente.

Letto e confermato alle ore 11.45.

IL SEGRETARIO GENERALE
Dott Alberto D'Arrigo

IL COMMISSARIO STRAORDINARIO
Dott. Salvatore Piazza

Registro di Settore n. 31 /2021	Deliberazione n. 31	29 MAR 2021

SI AFFIGGE, per la pubblicazione, all'Albo Provinciale, dal giorno 31 MAR 2021

al 15 APR 2021

Ragusa,_____

IL MESSO NOTIFICATORE

PUBBLICATA, mediante affissione all'Albo Provinciale, dal giorno_____al giorno _____

Ragusa,_____

IL MESSO NOTIFICATORE

CERTIFICATO DI PUBBLICAZIONE

Il Segretario sottoscritto certifica, su attestazione del messo notificatore, che la presente deliberazione è stata pubblicata, ai sensi dell'art.11, 1° comma L.R. 3 dicembre 1991, n. 44, mediante affissione di copia all'Albo Provinciale dal giorno festivo _____ al giorno _____, e che contro la stessa non è stata presentata opposizione.

Ragusa, _____

IL SEGRETARIO GENERALE

Registro di Settore n. 311../2021	Deliberazione n. 311.....	29 MAR 2021

LIBERO CONSORZIO COMUNALE DI RAGUSA
già Provincia Regionale di Ragusa

PROCEDURA PER LA GESTIONE DEGLI INCIDENTI INFORMATICI E DELLE VIOLAZIONI DEI DATI PERSONALI *(DATA BREACH)*

Sommario

INTRODUZIONE

La normativa vigente in materia di protezione dei dati personali prescrive ai titolari del trattamento di tutelare la riservatezza dei dati personali, al fine di evitare che ogni eventuale utilizzo non corretto degli stessi possa ledere i diritti e le libertà fondamentali dei soggetti interessati da tale trattamento.

Nell'ambito in cui opera il Libero Consorzio Comunale di Ragusa *già Provincia Regionale di Ragusa* in qualità di titolare del trattamento, tale onere risulta ancora più importante, dal momento che vengono trattate quotidianamente una pluralità di informazioni riferite ad un numero ingente di persone.

1. SCOPO DEL DOCUMENTO E CAMPO DI APPLICAZIONE

Il presente documento rappresenta il riferimento del Libero Consorzio Comunale di Ragusa (d'ora in avanti, per brevità definito *"LCC"*) per la regolamentazione della gestione delle violazioni dei dati personali – i cosiddetti *data breach* – che possono occorrere ai dati personali conservati e trattati dallo stesso. La corretta gestione degli incidenti di sicurezza permette di evitare o minimizzare la compromissione dei dati del LCC in caso di incidente, tutelando altresì i diritti e le libertà fondamentali dei soggetti interessati dalle attività di trattamento dei dati personali effettuate dalla stessa in qualità di titolare del trattamento; permette inoltre, attraverso l'analisi e la comprensione dei meccanismi di attacco e delle modalità utilizzate per la gestione dell'incidente, di migliorare continuamente la capacità di risposta agli incidenti.

Con specifico riferimento all'obbligo di cui all'art. 33 del Regolamento UE 2016/679 (d'ora in avanti semplicemente *"GDPR"*), il presente documento predispone un'apposita procedura finalizzata ad individuare quali siano le violazioni che ricadono nell'ambito della suddetta normativa, nonché i casi in cui il LCC deve notificare le violazioni dei dati personali *(data breach)* all'Autorità Garante per la protezione dei dati personali ed eventualmente agli interessati ai sensi dell'art. 34 del GDPR; inoltre, il documento descrive le misure atte a trattare e minimizzare i rischi per i diritti e le libertà delle persone interessate dallo specifico trattamento, nonché la documentazione da produrre in aderenza a quanto prescritto dalla normativa vigente in materia di protezione dei dati personali.

Pertanto, l'obiettivo della presente procedura è quello di definire delle precise istruzioni operative, da applicare ai soggetti che trattano dati personali per conto del LCC, nella sua qualità di titolare del trattamento. L'art. 32 del GDPR stabilisce, infatti, che devono essere approntate misure tecniche e organizzative adeguate a garantire un livello adeguato di sicurezza dei dati personali. Individuare, indirizzare e segnalare tempestivamente un incidente di sicurezza, specie se lo stesso comporta una violazione di dati personali, è espressione dell'adeguatezza delle misure implementate dal LCC e quindi del rispetto del principio di *accountability* in capo alla stessa nella sua qualità di titolare del trattamento, ai sensi dell'art. 5, par. 2, del Regolamento UE 2016/679.

L'ambito di applicazione è rappresentato da tutti i sistemi e gli archivi informativi del LCC– sia che trattino dati in formato cartaceo, che automatizzato – e vengono presi in considerazione incidenti che possono scaturire sia attraverso l'azione di un attacco portato da elementi esterni al LCC e, sia generati da un eventuale comportamento scorretto di un dipendente o di un collaboratore dello stesso.

2. RIFERIMENTI APPLICABILI

I documenti applicabili alla presente procedura vengono di seguito elencati:

- Regolamento UE 2016/679 *(General Data Protection Regulation)* del Parlamento Europeo e del Consiglio Europeo 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*;
- Decreto Legislativo 30 giugno 2003, n. 196 *"Codice in materia di protezione dei dati personali"*, per come novellato dal Decreto Legislativo 10 agosto 2018, n. 101;
- Provvedimenti, linee guida e pareri emanati ed adottati dall'Autorità Garante per la Protezione dei Dati Personali (GDPD), nonché dall'European Data Protection Board (EDPB);
- Schema internazionale *ISDP©10003:2020* per la valutazione della conformità al Regolamento europeo 2016/679;
- Prassi di Riferimento UNI/PdR 43:2018 *"Linee guida per la gestione dei dati personali in ambito ICT secondo il Regolamento UE 679/2016 (GDPR)"*;
- SGP 0901 Modello per la notifica di data breach al Garante;
- SGP 0902 Modulo per la comunicazione di data breach agli interessati;
- SGP 0103 Registro dei data breach.

3. TERMINI E DEFINIZIONI

Al fine di stabilire la terminologia di cui al presente documento, si riportano di seguito alcune definizioni tratte dall'articolo 4 del Regolamento UE 2016/679:

- *dato personale:* qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- *trattamento:* qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

- *limitazione di trattamento:* il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
- *profilazione:* qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
- *pseudonimizzazione:* il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
- *archivio:* qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
- *titolare del trattamento:* la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
- *responsabile del trattamento:* la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
- *destinatario:* la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;
- *terzo:* la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
- *consenso dell'interessato:* qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
- *violazione dei dati personali:* 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;

- *impresa:* la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;
- *gruppo imprenditoriale:* un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;
- *norme vincolanti d'impresa:* le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;
- *autorità di controllo:* l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;
- *autorità di controllo interessata:* un'autorità di controllo interessata dal trattamento di dati personali in quanto:
  - il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo;
  - gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure
  - un reclamo è stato proposto a tale autorità di controllo;
- *trattamento transfrontaliero:*
  - trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure
  - trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;
- *obiezione pertinente e motivata:* un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del Regolamento UE 2016/679, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme allo stesso Regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione;
- *servizio della società dell'informazione:* il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio:

  "qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi. Ai fini della presente definizione si intende per:

  - *«a distanza»: un servizio fornito senza la presenza simultanea delle parti;*

- *«per via elettronica»: un servizio inviato all'origine e ricevuto a destinazione mediante attrezzature elettroniche di trattamento (compresa la compressione digitale) e di memorizzazione di dati, e che è interamente trasmesso, inoltrato e ricevuto mediante fili, radio, mezzi ottici o altri mezzi elettromagnetici;*
- *«a richiesta individuale di un destinatario di servizi»: un servizio fornito mediante trasmissione di dati su richiesta individuale."*

per un elenco indicativo di servizi non contemplati da tale definizione, si rimanda all'allegato I della suddetta direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio;

- *organizzazione internazionale:* un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati;

4. LA VIOLAZIONE DEI DATI PERSONALI

Tutte le violazioni dei dati personali sono incidenti di sicurezza, ma non tutti gli incidenti di sicurezza sono necessariamente violazioni dei dati personali. L'obbligo di cui agli articoli 33 e 34 del Regolamento trova applicazione nei soli casi in cui la violazione riguardi *dati personali*, per come definiti nel capitolo terzo del presente documento.

Pertanto, un dato personale è *"qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale"*.

L'articolo 33 del Regolamento Europeo 2016/679 (GDPR), infatti, impone al titolare del trattamento di notificare all'autorità di controllo la violazione di dati personali *(data breach)* senza ingiustificato ritardo, e comunque entro 72 ore dal momento in cui ne viene a conoscenza. L'obbligo di notifica scatta se la violazione, ragionevolmente, comporta un rischio per i diritti e le libertà delle persone fisiche; qualora la violazione sia suscettibile di presentare un rischio elevato, inoltre, il titolare è tenuto a darne comunicazione all'interessato senza ingiustificato ritardo, ai sensi dell'art. 34 del GDPR. Ai sensi dell'articolo 33, paragrafo 1, del GDPR, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo. Ai sensi dell'articolo 33, paragrafo 2, del GDPR, ogni responsabile del trattamento è tenuto ad informare il titolare senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

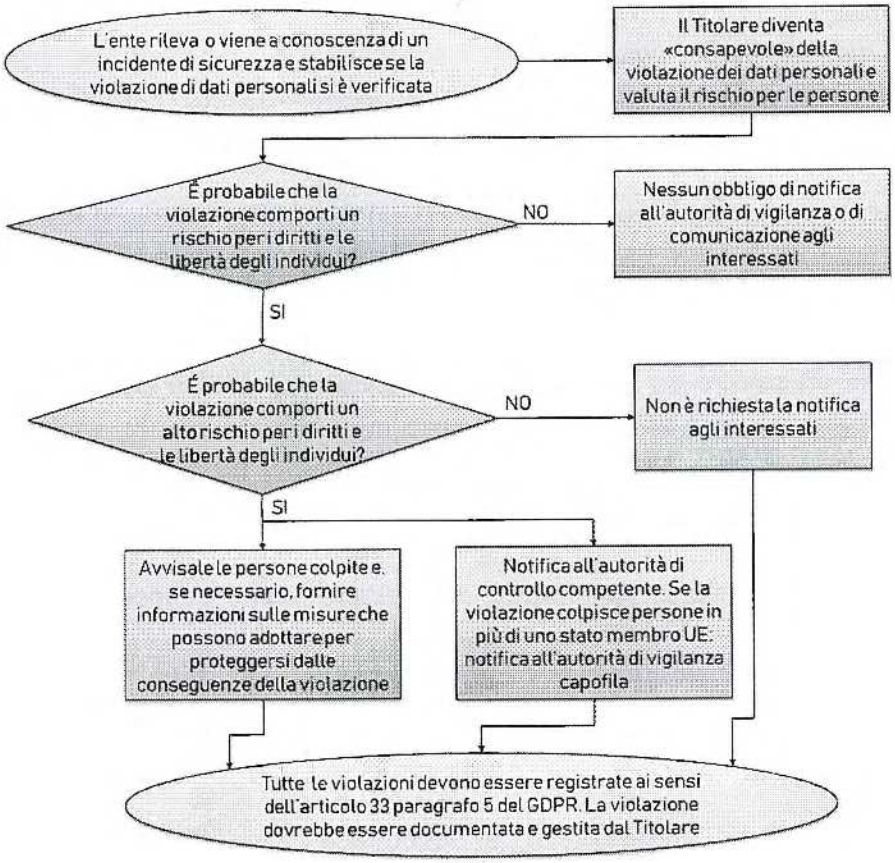
Nel caso in cui la notifica all'autorità di controllo non sia effettuata entro 72 ore, la stessa deve essere corredata dai motivi del ritardo; ne consegue l'importanza di rendere dimostrabile il momento della scoperta dell'incidente. Il mancato rispetto dell'obbligo di notifica, invece, pone l'autorità di controllo nella condizione di applicare le misure correttive a sua disposizione: l'esercizio dei poteri previsti dall'articolo 58 del GDPR (avvertimenti, ammonimenti, ingiunzioni, imposizione di limiti al

trattamento, ordine di rettifica, revoca di certificazioni, ordine di sospendere flussi dati) e/o l'imposizione di sanzioni amministrative pecuniarie ai sensi dell'articolo 83 GDPR.

Con il termine "violazione dei dati personali", definito al capitolo terzo del presente documento, 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"*. Pertanto, la violazione dei dati è un particolare tipo di incidente di sicurezza, per effetto del quale il titolare del trattamento non è in grado di garantire il rispetto dei principi prescritti dall'articolo 5 del GDPR applicabili al trattamento dei dati personali. Dunque, il titolare deve poter identificare preliminarmente l'incidente di sicurezza in genere, quindi comprendere che lo stesso abbia un impatto sulle informazioni, ed infine riconoscere che tra le informazioni coinvolte dall'incidente vi siano dati personali.

Il GDPR, all'articolo 33, paragrafo 5, prescrive al titolare di documentare *"qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio"*. Tale documentazione consente all'autorità di controllo di verificare il rispetto della norma. L'Organizzazione, a tal fine, ha predisposto – e mantiene costantemente aggiornato – l'apposito *Registro dei data breach*.

Di seguito, viene riportato uno schema di massima del flusso del processo descritto nella presente procedura operativa:



Si possono distinguere tre tipi di violazioni:

- violazione di *riservatezza*, ovvero quando si verifica una divulgazione o un accesso a dati personali non autorizzato o accidentale;
- violazione di *integrità*, ovvero quando si verifica un'alterazione di dati personali non autorizzata o accidentale;
- violazione di *disponibilità*, ovvero quando si verifica la perdita, l'inaccessibilità o la distruzione, accidentale o non autorizzata, di dati personali.

Una singola violazione dei dati personali potrebbe comprendere una o più tipologie.

5. VALUTAZIONE DEI RISCHI

Per comprendere quando notificare la violazione, è opportuno effettuare una valutazione dell'entità dei rischi per i diritti e le libertà fondamentali dei soggetti interessati, derivanti dall'incidente di sicurezza occorso agli archivi informativi organizzativi:

- *Rischio assente:* la notifica al Garante per la protezione dei dati personali non è obbligatoria.
- *Rischio presente:* è necessaria la notifica al Garante per la protezione dei dati personali.
- *Rischio elevato:* è necessaria anche la comunicazione della violazione ai soggetti interessati.

A tal proposito, si rammenta l'importanza di adottare le misure tecniche ed organizzative descritte in linea generale all'articolo 32 del Regolamento UE 2016/679 – il quale prescrive quanto di seguito riportato:

"Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

a) la pseudonimizzazione e la cifratura dei dati personali;
b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati."

I rischi per i diritti e le libertà degli interessati possono essere considerati "elevati" quando la violazione può, a titolo di esempio non esaustivo:

- coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;
- riguardare categorie particolari di dati personali, per come definite nell'articolo 9 del GDPR;
- comprendere dati che possano accrescere ulteriormente i potenziali rischi per i diritti e le libertà fondamentali dei soggetti interessati (es. dati di localizzazione, finanziari, relativi alle abitudini e preferenze);
- comportare rischi imminenti e con un'elevata probabilità di accadimento (es. rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito);
- impattare su soggetti che possono essere considerati vulnerabili per le loro particolari condizioni (es. minori, soggetti indagati, pazienti presso strutture sanitarie).

6. PROCESSO DI GESTIONE DELLA VIOLAZIONE DI DATI PERSONALI

Nel caso in cui venga accertata una violazione dei dati personali per come definita al capitolo 4 del presente documento il LCC segue gli steps del processo di gestione sotto descritti:

1. Acquisizione della notizia e informazione al titolare del trattamento
2. Analisi tecnica preliminare dell'evento
3. Valutazione approfondita della gravità dell'evento e notifica preliminare
4. Ulteriori indagini e notifiche integrative all'Autorità Garante
5. Eventuali altre segnalazioni dovute
6. Eventuale comunicazione della violazione agli interessati
7. Inserimento dell'evento nel Registro dei data breach

6.1. Acquisizione della notizia e informazione al titolare del trattamento

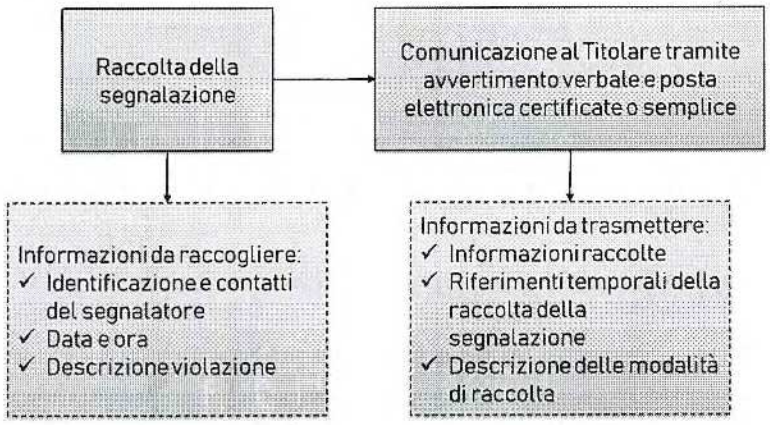
La segnalazione di un data breach può pervenire al titolare del trattamento sia dall'interno che esternamente; per esempio, per il tramite di un responsabile del trattamento oppure di uno dei soggetti interessati. A titolo esemplificativo e non esaustivo:

- Internamente:
  - Tramite il dipendente od il collaboratore del LCC che ne viene a conoscenza per primo
  - Tramite uno degli Amministratori di Sistema, ove sia un dipendente od un collaboratore del LCC
  - Tramite altri soggetti facenti parte dell'assetto organizzativo del titolare del trattamento
- Esternamente:
  - Tramite uno dei responsabili del trattamento
  - Tramite un organo pubblico

- Tramite uno dei soggetti interessati

Da qualunque fonte provenga la segnalazione, il personale del LCC comunica senza ingiustificato ritardo l'accaduto ai vertici apicali ed ai soggetti referenti per la protezione dei dati personali – nonché contestualmente al responsabile della protezione dei dati, ed all'Amministratore di Sistema ove opportuno. Quest'ultimo, nel caso di incidente che coinvolga i sistemi IT di sua competenza, provvede prima di tutto a ripristinare il normale funzionamento degli stessi nel più breve tempo possibile.

Ferme restando eventuali modalità di comunicazione verbali che possano rendersi necessarie al fine di avviare tempestivamente le opportune misure correttive, le comunicazioni interne devono avvenire a mezzo posta elettronica, anche al fine di permettere eventuali valutazioni *ex post* in merito alle tempistiche d'intervento.



Nel caso in cui il titolare del trattamento – nelle persone dei suddetti soggetti – venga a conoscenza dell'accaduto a mezzo posta elettronica ordinaria o certificata, le 72 ore entro cui effettuare l'eventuale notifica al Garante decorrono dall'orario di ricezione dell'e-mail. Nel caso in cui, invece, la segnalazione pervenga a mezzo posta ordinaria o posta raccomandata, le 72 ore decorrono dal momento in cui si riceve la comunicazione.

Visto quanto detto, è essenziale che vengano raccolte quanto prima tutte le informazioni possibili sull'accaduto, al fine di individuare il tipo di violazione e pertanto di valutare l'opportunità di effettuare la notifica al Garante: ciò perché, qualora la violazione non comporti rischi per nessuno dei tre parametri RID sopra elencati – *riservatezza, integrità, disponibilità* – il titolare del trattamento non ha l'obbligo di effettuare tale notifica.

L'articolo 33, paragrafo 1, del Regolamento UE 2016/679, infatti, chiarisce che non vi è obbligo di notifica della violazione quando è *"improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche"*. In ogni caso, anche il giudizio che determina l'improbabilità del rischio deve essere documentato nel *Registro dei data breach* del titolare del trattamento.

6.2. *Analisi tecnica preliminare dell'evento*

La responsabilità per quanto concerne la valutazione dell'accaduto è interamente a capo del titolare del trattamento, il quale viene opportunamente supportato da tutti i soggetti interni ed esterni al LCC che possano concorrere al raggiungimento di un quadro chiaro, ampio ed esaustivo dell'incidente.

Una volta appurato che l'evento segnalato si configura a tutti gli effetti quale *data breach ("analisi preliminare")*, si procede alla raccolta di tutte le operazioni necessarie alla valutazione dei rischi per i diritti e le libertà fondamentali degli interessati coinvolti. L'obiettivo di tale valutazione preliminare dell'evento è quello di raccogliere quante più informazioni possibili, così da individuare quali dei tre parametri RID sono stati compromessi.

Qualora dall'analisi preliminare non si abbia evidenza di possibili rischi per gli interessati, il titolare del trattamento provvede, avvalendosi del supporto del responsabile della protezione dei dati, alla compilazione del *Registro dei data breach*, avendo cura di documentare tutte le informazioni salienti al fine di evitare un altro futuro evento analogo. A tal proposito, è opportuno sottolineare l'importanza di registrare nel suddetto documento anche i cosiddetti *"near miss"*: gli eventi che – seppure non presentino i caratteri della violazione dei dati personali – avrebbero potuto compromettere i diritti e le libertà degli interessati se non fosse intercorsa una circostanza del tutto fortuita.

6.3. *Valutazione approfondita della gravità dell'evento e notifica preliminare*

In caso contrario – ovvero sia quando, in sede di analisi preliminare, venga rilevato un rischio per gli interessati – il titolare del trattamento passa ad effettuare un'accurata indagine interna *("analisi approfondita")*, nella quale deve accertare le cause della violazione, le sue conseguenze ed i relativi rimedi.

Si precisa, infatti, che l'articolo 33, paragrafo 4, del Regolamento UE 2016/679 prescrive che *"qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo"*. Pertanto, sarà fondamentale raccogliere il maggior numero di informazioni e, anche ove queste non siano ancora del tutto esaustive, effettuare – di concerto con il responsabile della protezione dei dati – la notifica cosiddetta *"preliminare"*: questa, che dev'essere immancabilmente inoltrata all'Autorità Garante per la protezione dei dati personali entro le 72 ore di cui sopra, deve riportare le informazioni minime richieste, per come descritto sul modulo per la notifica allegato alla presente procedura.

Nello specifico, dev'essere necessariamente individuato con assoluta certezza – ove possibile, entro le successive 12 ore e comunque senza ingiustificato ritardo – almeno quanto di seguito riportato:

- la tipologia, o le tipologie, della violazione con riferimento ai parametri di riservatezza, integrità e disponibilità;
- il momento in cui il titolare è venuto a conoscenza della violazione;
- ove possibile, quando è avvenuta la violazione;

- le modalità con cui il titolare è venuto a conoscenza della violazione;
- ove la notifica avvenga tardivamente, i motivi che hanno causato il ritardo;
- ove possibile, la causa della violazione;
- ove possibile, il volume approssimativo e le categorie di dati personali oggetto della violazione;
- ove possibile, il numero approssimativo e le categorie di interessati coinvolti nella violazione;
- i riferimenti del soggetto che il Garante potrà eventualmente contattare per ottenere maggiori informazioni circa la violazione.

Tutte le informazioni aggiuntive, come previsto dal suddetto articolo del GDPR, potranno essere fornite *"senza ulteriore ingiustificato ritardo"* all'Autorità Garante, mediante successive notifiche dette "integrative". Il data breach, pertanto, non potrà considerarsi chiuso se prima non si saranno comunicate al Garante tutte le informazioni di cui al suddetto *Modello di notifica al Garante*.

6.4. Ulteriori indagini e notifica integrativa all'Autorità Garante

Come sopra specificato, il Regolamento UE 2016/679 prevede che tutte le informazioni aggiuntive possano essere comunicate all'Autorità Garante per la protezione dei dati personali in fasi successive, senza ingiustificato ritardo.

Pertanto, il titolare del trattamento provvede ad avviare un'accurata attività investigativa interna, con l'obiettivo di formulare e documentare un quadro ampio ed esaustivo dell'accaduto. Nello specifico, le informazioni da raccogliere nel corso delle indagini – che serviranno quindi a compilare in ogni sua parte il suddetto *Modello di notifica al Garante*, ivi incluse eventuali informazioni che non è stato possibile fornire in fase preliminare – sono tutte le seguenti:

- i riferimenti di ulteriori soggetti coinvolti nel trattamento oggetto di violazione, oltre al ruolo svolto (contitolare o responsabile del trattamento, nonché eventuale rappresentante del titolare non stabilito nell'Unione Europea);
- informazioni di dettaglio sulla violazione, e nello specifico: una breve descrizione dell'incidente di sicurezza alla base della violazione; una breve descrizione delle categorie di dati personali coinvolte; una breve descrizione dei sistemi e delle infrastrutture IT coinvolti nell'incidente, ivi inclusa la loro ubicazione; una descrizione delle misure tecniche ed organizzative adottate per garantire la sicurezza dei dati, dei sistemi e delle infrastrutture coinvolti;
- un dettaglio delle possibili conseguenze della violazione sugli interessati, dal quale dedurre e motivare una stima della gravità della violazione;
- una descrizione delle misure tecniche e organizzative adottate, o di cui si prevede l'adozione, per porre rimedio alla violazione e ridurne gli effetti negativi, nonché di quelle adottate o previste al fine di prevenire simili violazioni future;
- ove applicabile, la data in cui è stata comunicata la violazione agli interessati, oppure in cui si prevede di effettuare la comunicazione;

- il numero di interessati a cui è stata comunicata la violazione, nonché il contenuto della stessa ed il canale scelto a tale scopo;
- eventuali altre informazioni, per come descritte alla Sez. H del *Modello di notifica al Garante*.

Nella redazione delle notifiche integrative al Garante, il titolare del trattamento – così come già per la notifica preliminare – si avvale del supporto del responsabile della protezione dei dati. In allegato alla presente procedura operativa, viene inserito il documento *SGP 0901 Modello notifica data breach* al Garante, in formato PDF editabile, per la notifica della violazione all'autorità di controllo. Una volta compilato, il modello deve essere sottoscritto dal rappresentante del titolare digitalmente con firma elettronica ed inviato, unitamente alla copia del documento d'identità del firmatario, via Posta Elettronica Certificata all'indirizzo *protocollo@pec.gpdp.it*. L'oggetto del messaggio deve contenere obbligatoriamente la dicitura *"NOTIFICA VIOLAZIONE DATI PERSONALI"*, ed opzionalmente la denominazione del titolare del trattamento.

6.5. *Eventuali altre segnalazioni dovute*

Già a decorrere dal momento in cui viene a conoscenza della violazione, il titolare del trattamento valuta l'opportunità di informare dell'accaduto altri organi competenti quali, a titolo esemplificativo e non esaustivo:

- Forze dell'Ordine, nel caso di incidente scaturito da comportamenti illeciti o fraudolenti;
- ove applicabile, il *Computer Security Incident Response Team (CSIRT)* italiano, in caso di incidenti informatici causati da attacchi cibernetici.

6.6. *Eventuale comunicazione della violazione ai soggetti interessati*

Ai sensi dell'articolo 34, paragrafo 1, del Regolamento UE 2016/679, *"quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo"*. L'obbligo di cui sopra non si applica, come specificato al paragrafo 3 dello stesso articolo del GDPR, quando sussista una delle seguenti condizioni:

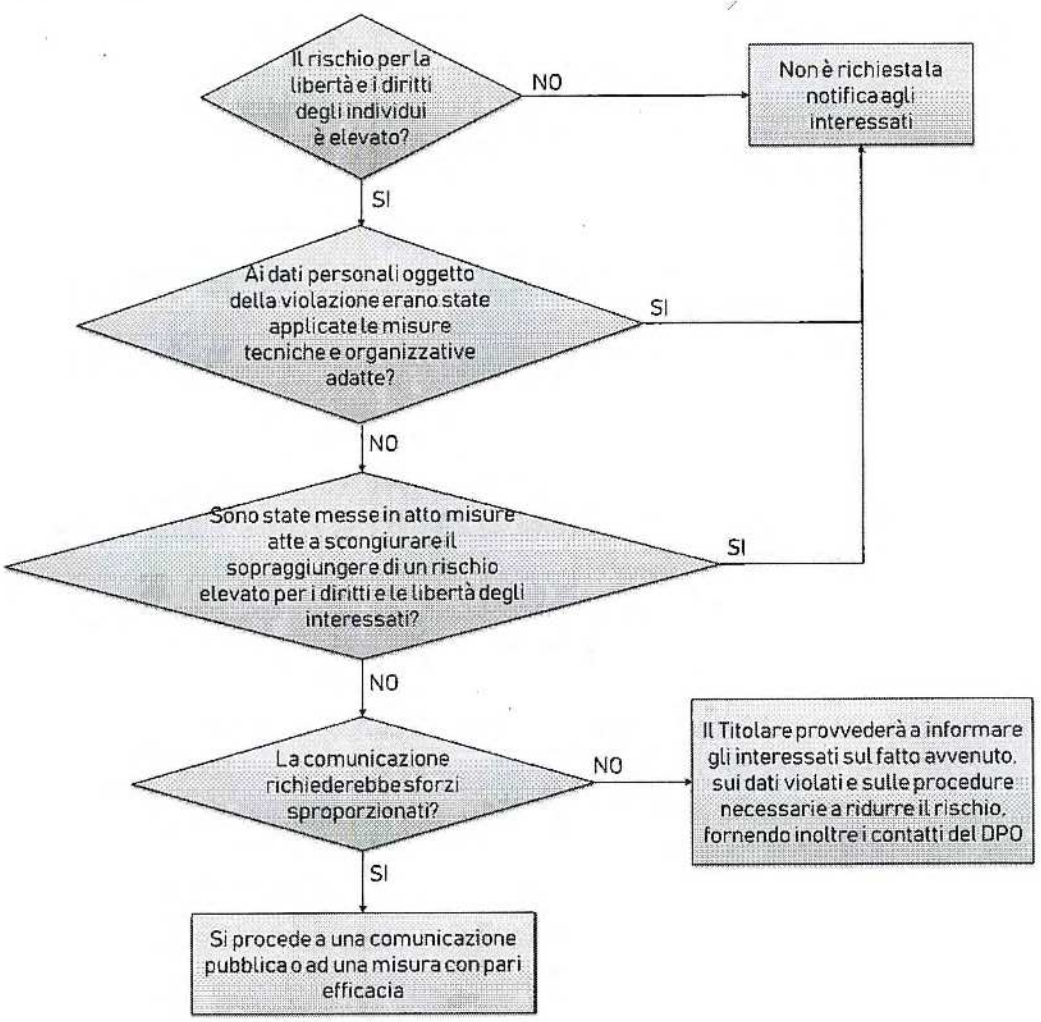
- il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
- il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
- la comunicazione agli interessati richiederebbe sforzi sproporzionati.

In quest'ultima fattispecie, il titolare del trattamento procede ad una comunicazione pubblica o ad una misura simile, tramite la quale gli interessati possano essere informati con analoga efficacia.

La comunicazione – per la quale il titolare si avvale del supporto del responsabile della protezione dei dati – descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali, riportando almeno le seguenti informazioni:

- il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- le probabili conseguenze della violazione dei dati personali;
- le misure adottate o di cui si propone l'adozione 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.

Per l'eventuale comunicazione della violazione ai soggetti interessati, il titolare del trattamento ha predisposto l'apposito *Modulo per la comunicazione data breach* agli interessati. In questo caso il titolare, di concerto con il responsabile della protezione dei dati, valuta caso per caso le modalità più opportune per l'invio di tale comunicazione, anche in considerazione dei recapiti dell'interessato a disposizione dell'Organizzazione.



6.7. *Inserimento dell'evento nel Registro dei data breach*

L'articolo 33, paragrafo 5, del Regolamento UE 2016/679, prescrive al titolare del trattamento – anche al fine di verificare il rispetto della normativa vigente in materia di protezione dei dati personali – di documentare *"qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio"*.

Pertanto, tutte le attività descritte ai punti precedenti devono essere documentate, tracciabili, ed il titolare del trattamento dev'essere in grado di fornire evidenza in merito alle stesse nelle sedi competenti. A tal fine, il titolare del trattamento ha predisposto l'apposito *Registro dei data breach*, il quale dev'essere compilato in ogni sua parte.

7. MONITORAGGIO E MIGLIORAMENTO CONTINUO

Le attività di trattamento effettuate dal titolare, al fine di mantenere costantemente l'aderenza alla normativa vigente, necessitano di verifiche periodiche atte a valutare e riesaminare le misure tecniche ed organizzative adottate – al fine di verificarne, con frequenza almeno annuale, l'efficacia e la corretta applicazione.

La procedura operativa di cui al presente documento, pertanto, viene considerata a tutti gli effetti parte integrante della documentazione soggetta a tali controlli periodici. A tal proposito, il titolare del trattamento – di concerto con il responsabile della protezione dei dati – effettua periodicamente attività di audit, mediante appositi strumenti di valutazione dell'aderenza alla normativa vigente in materia di trattamento dei dati personali, e del rischio cyber: tali controlli, infatti, consentono altresì di valutare, trattare e ridurre i rischi informatici e di sicurezza cibernetica – puntando inoltre ad individuare ed eliminare eventuali trattamenti che risultino potenzialmente lesivi dei diritti e delle libertà fondamentali degli interessati.

Il titolare, pertanto, si impegna affinché il LCC – ivi includendosi tutti i soggetti autorizzati a trattare dati personali – collabori attivamente per portare a termine con successo tali attività, in un'ottica di efficientamento organizzativo in generale. Ove necessario, peraltro, il titolare prevede il coinvolgimento dei responsabili del trattamento nelle attività sopra descritte.

Per quanto attiene alla presente procedura operativa, il titolare del trattamento – di concerto con gli Amministratori di Sistema ed il responsabile della protezione dei dati – valuta periodicamente gli incidenti riportati sull'apposito *Registro dei data breach* ed analizza le evidenze raccolte, eventualmente elaborando le opportune misure di mitigazione affinché tale tipologia di incidente non possa più verificarsi. Inoltre, nel caso in cui gli stessi soggetti rilevino la ciclicità di alcuni accadimenti, effettuano una analisi più approfondita al fine di individuare le cause di tale ricorsività degli avvenimenti, documentare le evidenze raccolte ed elaborare le idonee misure di mitigazione affinché tale tipologia di incidente non possa più verificarsi.

8. RESPONSABILITÀ IN CAPO A TITOLARE, RESPONSABILE E DPO

La responsabilità generale, per tutto quanto concerne l'applicazione della presente procedura, spetta al titolare del trattamento – il quale viene opportunamente coadiuvato dal responsabile della protezione dei dati, secondo quanto disposto dalla normativa vigente in materia di protezione dei dati personali.

Per quanto attiene alla responsabilità del trattamento dei dati personali, l'articolo 82 del Regolamento UE 2016/679 stabilisce che *"Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento"*. Pertanto, il titolare del trattamento riconosce di rispondere per il danno cagionato dal trattamento che violi quanto previsto dal GDPR.

Ad ogni modo, anche il soggetto individuato quale responsabile del trattamento ai sensi dell'articolo 28 dello stesso Regolamento, risponde in caso di inadempimento degli obblighi ovvero qualora abbia agito in modo difforme o contrario rispetto alle istruzioni fornite dal titolare del trattamento. Inoltre, ai sensi del suddetto articolo 28 – e nello specifico del paragrafo 10 di detto articolo – se un responsabile del trattamento viola il Regolamento, determinando le finalità e i mezzi del trattamento, è considerato un titolare autonomo: ne consegue, in altre parole, che è soggetto a tutti gli effetti alle responsabilità in capo al titolare di cui agli articoli 82, 83 e 84 del GDPR.

Tutto ciò premesso, la responsabilità del trattamento resta in capo al titolare e non è in alcun modo delegabile, anche in virtù del principio di responsabilizzazione di cui all'articolo 5 , paragrafo 2, del Regolamento UE 2016/679; quindi, è il titolare che dev'essere in grado di dimostrare il perseguimento dei principi applicabili alla protezione dei dati personali e l'adozione di misure tecniche ed organizzative adeguate al rischio, oltre alla non imputabilità alla propria condotta di eventuali danni a terzi, al fine di evitare di incorrere nelle sanzioni previste.

9. GESTIONE DEL DOCUMENTO E DELLE RELATIVE COMUNICAZIONI

Il titolare del trattamento – con il supporto del responsabile della protezione dei dati, ove necessario – comunica con l'ufficio competente, all'interno del LCC, in relazione alla violazione di dati personali occorsa. Ove necessario, ciò può anche comportare la necessità di effettuare uno o più incontri – ovvero riunioni anche in modalità telematica, o colloqui telefonici – atti ad effettuare le dovute valutazioni del caso: nell'ambito di tali attività, il titolare del trattamento – nonché i soggetti coinvolti nel processo ed il responsabile della protezione dei dati – tengono in considerazione anche le tempistiche individuate nella presente procedura.

La figura del responsabile della protezione dei dati, pertanto, si impegna a supportare il titolare del trattamento al fine di gestire le attività di cui alla presente procedura in maniera coordinata e strutturata – ovvero per garantire in modo efficace ed efficiente il rispetto dei principi e delle disposizioni di cui alla normativa vigente in materia di protezione dei dati personali. A tal proposito, il responsabile della protezione dei dati dovrà essere adeguatamente informato – nonché ricevere ampia ed esaustiva documentazione – dal titolare del trattamento nell'ambito della presente procedura, configurandosi altresì come punto di contatto per l'autorità di controllo ai sensi e per gli effetti delle disposizioni di cui alla Sezione 4 del Capo IV del Regolamento UE 2016/679.

Nello specifico, è opportuno che tutte le comunicazioni inerenti all'applicazione della presente procedura – ivi incluse la gestione delle comunicazioni tra il titolare del trattamento ed i soggetti interessati – prevedano il coinvolgimento del responsabile della protezione dei dati, al fine di ricevere pieno supporto dallo stesso. Inoltre, anche al fine di effettuare valutazioni *ex post* circa le tempistiche relative alla gestione delle fasi descritte in seguito, il titolare del trattamento adotta idonei strumenti atti a determinare la data e l'ora delle comunicazioni inerenti alla gestione della violazione.

Il responsabile per il presente documento è il titolare del trattamento, il quale deve controllare e, se necessario, aggiornare la procedura con frequenza almeno annuale. Tale procedura deve essere altresì diffusa a tutti i dipendenti del LCC del titolare che siano autorizzati al trattamento dei dati personali per conto del titolare: ferme restando le rispettive mansioni, ed in funzione delle relative aree organizzative di competenza, ove richiesto tali soggetti dovranno fornire pieno supporto al titolare del trattamento nell'esecuzione delle attività descritte dalla presente procedura operativa.

Si allega il seguente documento:

- Allegato "A" modello per la comunicazione della violazione di dati personalil.

ALLEGATO "A"

LIBERO CONSORZIO COMUNALE DI RAGUSA
già Provincia Regionale di Ragusa

MODULO PER LA COMUNICAZIONE DI VIOLAZIONE DEI DATI PERSONALI

effettuata ai sensi dell'articolo 34 del Regolamento UE 2016/679

Titolare del trattamento e responsabile della protezione dei dati

Libero Consorzio Comunale di Ragusa *già Provincia Regionale di Ragusa* con sede in Viale del Fante 10 – 97100 Ragusa
C.F./P.IVA: 80000010886 – Tel: (+39) 0932 675111 – Fax: (+39) 0932 248825 – PEC: protocollo@pec.provincia.ragusa.it
Responsabile della Protezione dei Dati (DPO) contattabile all'indirizzo di posta elettronica: dpo@provincia.ragusa.it.

Riferimenti della comunicazione

Comunicazione di violazione dei dati personali inoltrata a _____ ,
C.F. _____ , per mezzo del seguente indirizzo e-mail/numero di telefono del soggetto interessato _____ .

Dettaglio della comunicazione

Gentile Signore/Signora, il suddetto titolare del trattamento è spiacente di informarLa di essere venuto a conoscenza, in data ___/___/_____ , di una violazione dei dati personali che La riguardano. Conseguentemente a tale violazione, i Suoi dati personali potrebbero essere stati: ○ *Divulgati* ○ *Distrutti* ○ *Persi* ○ *Modificati* ○ *Consultati* da parte di soggetti non autorizzati.

Conseguenze della violazione

Il titolare del trattamento, in riferimento alla violazione dei dati personali che La riguardano, ha individuato le seguenti possibili conseguenze *(art. 34, par. 2, del Regolamento UE 2016/679)*:

_____
_____
_____ .

Misure adottate e pianificate

Il titolare del trattamento, al fine di porre rimedio alla violazione dei dati personali ed attenuarne i possibili effetti negativi, ha:

- ○ Adottato le seguenti misure:

  _____
  _____
  _____ ;

- ○ Pianificato l'adozione delle seguenti misure:

  _____
  _____
  _____ .

Luogo e data: _____ , ___/___/_____ Timbro e Firma: _____