ORDINE DELLA PROFESSIONE DI OSTETRICA
DELLA PROVINCIA DI SASSARI
Viale Umberto, 112 – 07100 SASSARI
Tel. 079/271119 – Fax 079/275551
E-mail segreteria@ostetrichesassari.it
PEC collegioostetrichessot@pec.collegioostetrichessot.it
Sito internet www.ostetrichesassari.it

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

INDICE DELLE REVISIONI

Revisione	Data	Descrizione	Verifica	Approvazione
v1.0	Maggio 2020			

ORDINE DELLA PROFESSIONE DI OSTETRICA
DELLA PROVINCIA DI SASSARI
Viale Umberto, 112 – 07100 SASSARI
Tel. 079/271119 – Fax 079/275551
E-mail segreteria@ostetrichesassari.it
PEC collegioostetrichessot@pec.collegioostetrichessot.it
Sito internet www.ostetrichesassari.it

SOMMARIO

1. PREMESSA/SCOPO

La presente procedura descrive le attività e le registrazioni da produrre circa il processo di gestione delle violazioni di Dati personali (c.d. Data Breach) che dovessero verificarsi, al fine di permettere all'Ordine delle Ostetriche di Sassari di adempiere agli obblighi di notificazione e di comunicazione imposti, rispettivamente, dall'art. 33 del Regolamento UE 2016/679 e dall'art. 34 del Regolamento UE 2016/679 (di seguito anche "GDPR").

2. FONTI NORMATIVE

Di seguito sono riportate le fonti normative applicabili nei casi di violazione dei dati personali, anche potenziale:

- Art. 33 Regolamento UE 2016/679 "Notifica di una violazione dei Dati personali all'Autorità Garante"
- Art. 34 Regolamento UE 2016/679 "Comunicazione di una violazione dei Dati personali all'interessato"
- WP 250 ENG - Guidelines on Personal data breach notification under Regulation 679

3. TERMINI E DEFINIZIONI

Nella tabella seguente sono riportati i termini e le definizioni di cui all'art. 4 Regolamento UE 2016/679.

Termine	Definizione
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.
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.

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.
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.
Dati genetici	I Dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione.
Dati biometrici	I Dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.
Dati relativi alla salute	I Dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.
Autorità di Controllo	L'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51.

Tabella 1 – Termini e definizioni (art. 4 Regolamento UE 2016/679)

4. REFERENTE (PRIVACY) DEL PROCESSO

Il Titolare del trattamento (l'Ordine delle Ostetriche nella persona del Referente Privacy), al fine di garantire un intervento tempestivo non appena si manifesti, o anche solo si sospetti, una violazione di Dati personali, ha ritenuto opportuno nominare espressamente un Referente Privacy, il quale lo supporti nella gestione e dunque nell'adempimento di tutti gli incombenti previsti dalla normativa applicabile nei casi di violazione dei dati (anche potenziale).

Entrambi insieme valuteranno:

- la natura e l'entità della potenziale violazione/ violazione dei Dati personali;
- l'impatto della violazione dati dei Dati personali;
- le misure da adottare per arginare gli effetti dannosi della violazione medesima;
- la necessità di notifica al Garante;
- la necessità della notifica agli interessati.

5. DEFINIZIONE DI DATA BREACH

Una "**violazione dei Dati personali**" (art. 4, par. 12 GDPR) è:

- **natura della violazione:**
  - **accidentale;**
  - **illecita;**
- **conseguenza sui dati:**
  - **distruzione;**
  - **perdita;**
  - **modifica;**
  - **divulgazione non autorizzata;**
  - **accesso ai dati da parte di soggetti non autorizzati;**
- **conseguenze sugli interessati:**
  - **danni morali o immateriali;**
  - **perdita del controllo dei dati e conseguenti perdite economiche;**
  - **discriminazioni;**
  - **furto d'identità e frode;**
  - **danno reputazionale;**
  - **ecc.**

ALCUNI ESEMPI DI VIOLAZIONE DEI DATI:

- computer, smartphone, memorie e dischi USB rubati persi o lasciati temporaneamente incustoditi, oppure smaltiti in modo inadeguato;
- allagamento o incendi degli archivi cartacei;
- furto smarrimento o condivisione della password o di altre informazioni di autenticazione;
- negligenza dei soggetti che trattano i Dati personali dell'ordine nell'utilizzare password semplici e facilmente identificabili;
- negligenza nel divulgare a soggetti non autorizzati informazioni protette e riservate o superficialità nel trattare e trasmettere Dati personali;

- abuso di privilegi in ambiente di rete che possono determinare modifiche ai Dati personali o installazione di software non autorizzato;
- furto di documenti cartacei contenenti informazioni personali o riservate lasciati incustoditi sulla scrivania o alla fotocopiatrice oppure smaltiti in modo inadeguato;
- inadeguate misure di sicurezza e di protezione che lasciano i sistemi vulnerabili e consentono attacchi di hacker o di organizzazioni esterne attuati mediante software che bypassano i sistemi di sicurezza, es. firewall, per accedere ai data base aziendali.

Una violazione dei Dati personali è quindi un incidente di sicurezza che interessa un insieme di Dati personali.

Le violazioni dei Dati personali possono essere classificate in base alle 3 dimensioni di RISERVATEZZA, INTEGRITÀ E DISPONIBILITÀ:

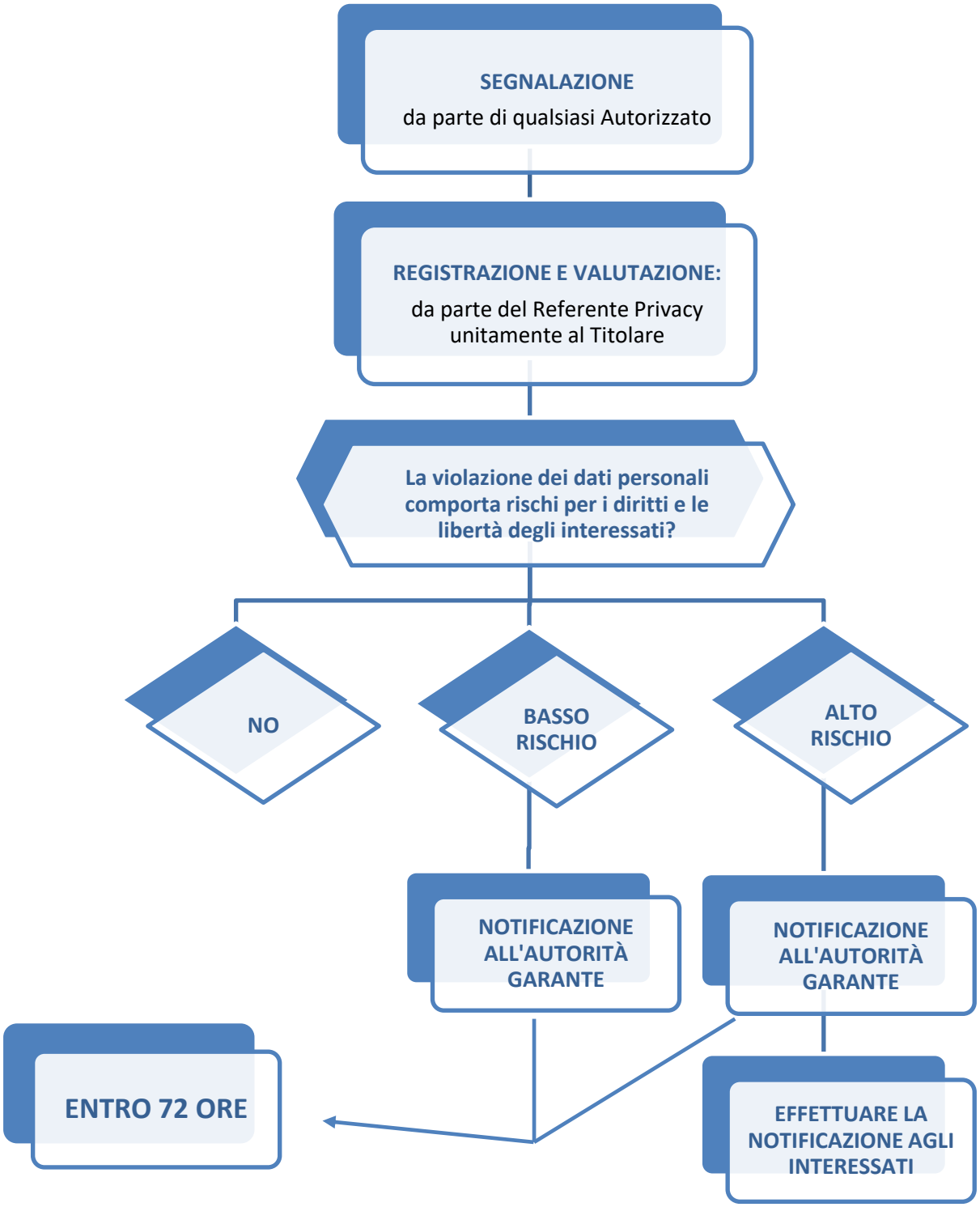
- **“VIOLAZIONE DELLA RISERVATEZZA" si ha in caso di divulgazione o accesso non autorizzato o accidentale ai Dati personali;**
- **"VIOLAZIONE DELLA DISPONIBILITÀ" si ha in caso di perdita accidentale o non autorizzata di accesso o distruzione di Dati personali;**
- **"VIOLAZIONE DELL'INTEGRITÀ" si ha in caso di alterazione non autorizzata o accidentale dei Dati personali.**

A seconda delle circostanze, un Data Breach può riguardare la riservatezza, la disponibilità e l'integrità dei Dati personali allo stesso tempo, nonché qualsiasi combinazione di queste dimensioni.

6. FLOWCHART PROCEDURA EVENTI DI DATA BREACH

Il seguente diagramma di flusso riporta la rappresentazione grafica della procedura di segnalazione, registrazione e notificazione e comunicazione delle violazioni dei Dati personali.

ORDINE DELLA PROFESSIONE DI OSTETRICA
DELLA PROVINCIA DI SASSARI
Viale Umberto, 112 – 07100 SASSARI
Tel. 079/271119 – Fax 079/275551
E-mail segreteria@ostetrichesassari.it
PEC collegioostetrichessot@pec.collegioostetrichessot.it
Sito internet www.ostetrichesassari.it



7. PROCEDURA DI GESTIONE DELLE VIOLAZIONE DEI DATI PERSONALI

7.1. SEGNALAZIONE

Il paragrafo 1 dell'articolo 33 del GDPR stabilisce che:

> *"In caso di violazione dei Dati personali, il Titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei Dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo".*

Il paragrafo 1 dell'articolo 34 del GDPR stabilisce che:

> *"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'Ordine delle Ostetriche di Sassari ha individuato le seguenti categorie di soggetti che possono segnalare violazioni dei Dati personali:

- dipendenti/consigliere/collaboratori che, nell'ambito della propria mansione lavorativa/rapporto di collaborazione effettuano attività di trattamento dei Dati personali del Titolare (l'Ordine);
- Amministratori di Sistema che gestiscono e mantengono l'infrastruttura IT del Titolare (software house, informatico IT, gestori del sito);
- Responsabili del trattamento (*ex* art. 28 GDPR) che effettuano attività di trattamento dei Dati personali per conto del Titolare (fornitori che per conto del Titolare trattano Dati personali, commercialista RSPP, consulente del lavoro ecc. vd. *"elenco responsabili esterni"*);
- tutti coloro che potrebbero avvedersi della violazione di Dati personali di cui la Titolarità è in capo all'Ordine delle Ostetriche di Sassari;

OBBLIGO DEI DIPENDENTI/COLLABORATORI/MEMBRI DEL CONSIGLIO DELL'ORDINE IN CASO DI VIOLAZIONE DEI DATI

Questi soggetti se sospettano o rilevano di una violazione dei Dati personali devono IMMEDIATAMENTE:

- Mettere in atto contromisure atte a contenere e limitarne l'impatto e se possibile arrestare la violazione, solo se si è in grado.
- Segnalare l'accaduto immediatamente attraverso un'e-mail al Referente Privacy, segnalando la possibile violazione/violazione accorsa.
- Fare seguire all'e-mail una telefonata che assicuri un tempestivo riscontro da parte del Referente Privacy.
- In caso di mancata risposta o mancata attivazione da parte del Referente Privacy entro 15 minuti, provvedere all'invio dell'e-mail al Titolare del trattamento o al DPO.
- Fare seguire all'e-mail una telefonata che assicuri un tempestivo riscontro da parte del Titolare o del DPO.
- In ogni caso, assicurarsi dell'effettivo riscontro da parte del soggetto coinvolto e contattato e reiterare la segnalazione per il tramite di e-mail o telefonate sino a che non abbia ottenuto risposta e conferma di presa in carico della segnalazione.

Il personale che rileva la violazione di Dati personali deve porre particolare attenzione sulla necessità di conservare e non alterare nessuna prova della violazione per rendere possibili ulteriori successive indagini.

7.2. REGISTRAZIONE E VALUTAZIONE

Il **Referente Privacy**, nel momento in cui è informato circa una violazione dei Dati personali, **ha la responsabilità di:**

- avvisare IMMEDIATAMENTE il DPO e il Titolare del trattamento;
- interfacciarsi con il soggetto che ha effettuato la segnalazione e raccogliere tutte le informazioni necessarie per analizzare l'evento occorso;
- determinare, unitamente al Titolare del Trattamento e con il supporto e la supervisione del DPO, le necessarie misure di mitigazione per la gestione della violazione occorsa o ancora in corso;
- valutare, entro 72 ore dalla conoscenza della violazione, unitamente al Titolare, se sia necessario o meno procedere con la notifica al Garante e agli interessati coinvolti;
- registrare l'accaduto nel Registro delle violazioni.

Il Referente Privacy dovrà riportare nel "Registro delle Violazioni" le seguenti informazioni:

Informazioni	Descrizione
• Origine segnalazione	• Dipendente/collaboratore • Amministratore di Sistema • Responsabile del trattamento
• Date e ora segnalazione	• Data e ora in cui la violazione è stata rilevata (tale indicazione è molto importante poiché dal momento in cui vi è consapevolezza di una violazione partono le 72 ore entro cui deve essere effettuata l'eventuale notificazione all'Autorità Garante
• Descrizione natura violazione	• Dispositivi oggetto di violazione • Tipologia di violazione: - Violazione della riservatezza dei Dati personali - Violazione della disponibilità dei Dati personali - Violazione dell'integrità dei Dati personali • Categorie interessati • Numero interessati • Categorie di Dati personali
• Indicazione e descrizione dei possibili rischi per i diritti e le libertà degli interessati	Indicare gli effetti negativi per gli interessati derivanti dalla violazione: • la perdita di controllo sui propri Dati personali • la limitazione dei loro diritti • discriminazione • furto d'identità o frode • perdita finanziaria • danno alla reputazione • perdita di riservatezza dei Dati personali protetti dal segreto professionale • qualsiasi altro significativo svantaggio economico o sociale
• Valutazione della probabilità di realizzazione dei rischi per i diritti e le libertà degli interessati	Indicare la probabilità di realizzazione degli effetti negativi per gli interessati derivanti dalla violazione, anche alla luce delle misure di sicurezza in essere: • probabilità BASSA (notificazione all'Autorità Garante) • probabilità ALTA (notificazione all'Autorità Garante e comunicazione agli interessati)
• Misure adottate/di cui si propone l'adozione per contrastare la violazione e/o attenuarne i possibili effetti negativi	Descrivere le misure adottate/che si propone di adottare

Tabella 2 – Informazioni da inserire nel Registro delle violazioni dei Dati personali

7.3. NOTIFICAZIONE ALL'AUTORITÀ GARANTE

Il Referente Privacy, unitamente al Titolare, nel valutare se fare o meno la notifica al Garante deve tenere in considerazione sia la probabilità che la gravità del rischio per i diritti e le libertà delle persone, in ragione della natura, sensibilità e volume dei dati, numero degli individui coinvolti, facilità di identificazione, gravità e conseguenze degli stessi.

Non è richiesta notifica se la violazione non costituisce un probabile rischio per l'individuo.

Per esempio, qualora i dati violati siano criptati, la chiave non sia compromessa e sia stata generata con soluzioni software non a disposizione di qualsiasi persona non autorizzata ad accedervi, rendendo i dati almeno in linea di principio incomprensibili, se esiste una copia di backup non è necessaria la notifica. È evidente che se la chiave di crittografia è compromessa o il software di crittografia o il suo algoritmo è vulnerabile, esiste un rischio per i diritti e le libertà delle persone fisiche e la notifica può essere richiesta.

Il paragrafo 3 dell'articolo 33 del GDPR stabilisce **che la notificazione all'Autorità Garante deve**:

- descrivere la natura della violazione dei Dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei Dati personali in questione;
- comunicare il nome e i dati di contatto del DPO o di altro punto di contatto presso cui ottenere più informazioni;
- descrivere le probabili conseguenze della violazione dei Dati personali;
- descrivere 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.

Nel caso di violazioni di Dati personali che presentano rischi per i diritti e le libertà degli interessati coinvolti, il Referente Privacy deve effettuare la notificazione all'Autorità Garante, riportando tutte le informazioni richieste dal suddetto art. 33 comma 3 e utilizzando l'apposito Modulo Data Breach[1], all'uopo diffuso dall'Autorità Garante per la protezione dei Dati personali.

[1] Si veda modulo allegato.

La notifica deve essere inviata al Garante tramite posta elettronica all'indirizzo **protocollo@pec.gpdp.it** e deve essere sottoscritta digitalmente (con firma elettronica qualificata/firma digitale) ovvero con firma autografa.

In quest'ultimo caso la notifica deve essere presentata unitamente alla copia del documento d'identità del firmatario.

7.4. COMUNICAZIONE AGLI INTERESSATI

Se la violazione dei Dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Referente Privacy unitamente al Titolare e con la supervisione del DPO, comunica la violazione all'interessato senza ingiustificato ritardo, per il tramite di detta comunicazione si dovrà:

- comunicare il nome e i dati di contatto del responsabile della protezione dei dati (DPO), se designato, o di altro punto di contatto presso cui ottenere più informazioni;
- descrivere le probabili conseguenze della violazione dei Dati personali;
- descrivere 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.

Non è richiesta la comunicazione all'interessato in presenza di 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;
- detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

8. VIOLAZIONE DELLA PROCEDURA

Qualora il Titolare, anche a seguito di violazioni e perdita di riservatezza dei Dati personali ovvero di *data breach* in genere, che provochino danno all'Ordine, rilevi comportamenti che possono mettere a rischio la prosecuzione delle attività o esserne causa in quanto non conformi alle indicazioni della presente policy, il Titolare (il consiglio) si riserva la possibilità di agire nei confronti di coloro che possano esserne ritenuti

responsabili, riservandosi di poter addebitare loro i costi che ne derivano oltre che la possibilità di intraprendere procedimenti disciplinari sanzionatori secondo le norme del CCNL di volta in volta applicato.