Collegio Provinciale dei Geometri e Geometri Laureati di Caltanissetta
Via F. De Roberto, 79 – 93100 Caltanissetta
c.f. 80004260859 – tel. 0934/22593
Mail: sede@collegio.geometri.cl.it - **PEC:** collegio.caltanissetta@geopec.it

# # #

PIANO DI RISPOSTA PER LA GESTIONE DELLE VIOLAZIONI DELLA SICUREZZA DEI DATI

# # #

ADEMPIMENTI da effettuare in caso di DATA BREACH

# # #

PREMESSA

L'Ente ai sensi del Regolamento Europeo 2016/679, è tenuto a mantenere sicuri i dati personali trattati nell'ambito delle proprie attività e ad agire senza ingiustificato ritardo in caso di violazione dei dati stessi

Il presente Piano predispone le azioni da attuare nell'eventualità in cui si presentino violazioni concrete, potenziali o sospette di dati personali, al fine di evitare rischi per i diritti e le libertà degli interessati, nonché danni economici all'ente e riscontrare nei tempi e nei modi previsti dalla normativa europea l'Autorità Garante e gli interessati.

Le sanzioni previste dal GDPR per l'omessa notifica di un Data Breach all'Autorità di Controllo o omessa comunicazione agli interessati o entrambi gli adempimenti, nei casi in cui siano soddisfatti i requisiti di cui agli artt. 33 e 34 GDPR, può comportare l'applicazione in capo all'ente di una sanzione amministrativa pecuniaria fino a 10 milioni di euro che può essere anche accompagnata da una misura correttiva ai sensi dell'art. 58 c. 2.

A CHI E' RIVOLTA QUESTE PROCEDURA ?

Questa procedura è deve essere applicata da tutti i soggetti che a qualsiasi titolo trattano dati personali di competenza del Titolare del trattamento quali:

- i lavoratori dipendenti, nonché coloro che a qualsiasi titolo - e quindi a prescindere dal tipo di rapporto intercorrente - abbiano accesso ai dati personali trattati nel corso del proprio impiego per conto del Titolare del trattamento;
- qualsiasi soggetto (persona fisica o persona giuridica) che, in ragione del rapporto contrattuale in essere con il Titolare del trattamento abbia accesso ai suddetti dati e agisca in qualità di Responsabile del trattamento ex art. 28 GDPR o di autonomo Titolare;

Tali soggetti devono essere debitamente informati dell'esistenza della presente procedura, mediante metodi e mezzi che ne assicurino la comprensione.

Il rispetto della presente procedura è obbligatorio per tutti i soggetti coinvolti e la mancata conformità alle regole di comportamento previste dalla stessa potrà comportare provvedimenti disciplinari a carico dei dipendenti inadempienti ovvero la risoluzione dei contratti in essere con terze parti inadempienti, secondo le normative vigenti in materia.

A QUALI TIPI DI DATI SI APPLICA QUESTA PROCEDURA ?

Questa procedura si riferisce a:

- dati personali trattati "da" o "per conto" del Titolare del trattamento, in qualsiasi formato (inclusi documenti cartacei) e con qualsiasi mezzo;
- dati personali conservati, comunicati, rielaborati o trattati con qualsiasi modalità o sistema.

Per «***dato personale***» si intende: 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.

COS'È UNA VIOLAZIONE DEI DATI PERSONALI (DATA BREACH) ?

Art. 4, punto 12, del Regolamento 679/2016:"**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*

Un data breach può essere classificato in base a **tre principi della sicurezza** delle informazioni:

violazione della disponibilità	Violazione della integrità	Violazione della riservatezza
• distruzione • perdita non autorizzata di dati	• modifica non autorizzata di dati personali	• divulgazione • accesso non autorizzato di dati personali

Un data breach può anche riguardare contemporaneamente la riservatezza, l'integrità e òa disponibilità dei dati personali oppure una combinazione delle stesse.

Distruzione non autorizzata	•indisponibilità definitiva di dati personali degli interessati con impossibilità di ripristino degli stessi
Perdita	•perdita di un supporto fisico di memorizzazione contenente dati personali degli interessati oppure documenti cartacei
Modifica non autorizzata	•modifiche dei dati degli interessati effettuate da incaricati non autorizzati •modifiche con finalità fraudolente eseguite eseguite dagli incricati autorizzati
Divulgazione non autorizzata	•distribuzione non autorizzata o illecita dei dati personali degli interessati verso terzi anche non precisamente identificabili
Accesso non autorizzato	•accesso non autorizzato o improprio a dati degli interessati •accesso ai dati avvenuto al di fuori dei processi di trattamento dei dati previsti e autorizzati

Le violazioni di dati personali possono verificarsi in un ampio numero di casi che possono includere, ad esempio:

- divulgazione di dati confidenziali a persone non autorizzate;
- perdita o furto di dati o di strumenti nei quali i dati sono memorizzati;
- perdita o furto di documenti cartacei;
- infedeltà del dipendente (ad esempio: una persona interna che avendo autorizzazione ad accedere ai dati ne produce una copia che divulga);
- **accesso abusivo ad un sistema informatico o telematico** protetto da misure di sicurezza. Attenzione perche tale comportamento potrebbe configurarsi anche il reato penale previsto e punito dall'art. 615-ter del codice penale che prevede un'aggravante quando il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri, o con violazione dei doveri inerenti alla funzione o al servizio, o con abuso della qualità di operatore del sistema. La Corte di Cassazione a sezioni Unite con la sentenza 18 maggio 2017 n. 41210 ha ritenuto che commette il reato un pubblico ufficiale o l'incaricato di pubblico servizio che, munito di password di accesso al sistema, pur essendo abilitato e pur non violando le prescrizioni formali impartite dal titolare, vi acceda per finalità diverse da quelle di ufficio realizzando un c.d. sviamento di potere o si mantenga nel sistema per ragioni ontologicamente estranee e comunque diverse rispetto a quelle per le quali, soltanto, la facoltà di accesso gli è attribuita.
- casi di pirateria informatica;

- banche dati alterate o distrutte senza autorizzazione rilasciata dal relativo "owner";
- virus o altri attacchi al sistema informatico o alla rete;
- violazione di misure di sicurezza fisica (ad esempio: forzatura di porte o finestre di stanze di sicurezza o archivi, contenenti informazioni riservate);
- smarrimento di pc portatili, devices o attrezzature informatiche;
- invio di e-mail contenenti dati personali a erroneo destinatario.

PERCHE' E' IMPORTANTE SEGUIRE QUESTA PROCEDURA ?

Un data breach può avere **conseguenze** particolarmente gravi, quali, ad esempio:

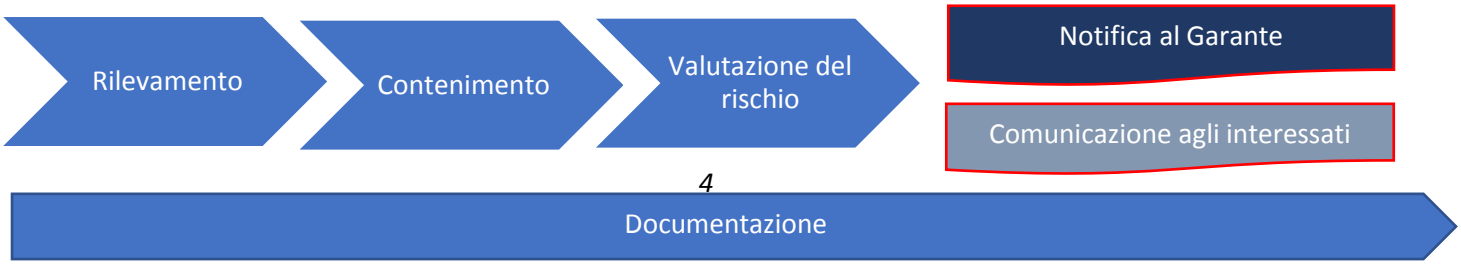
- Perdita del controllo sui dati personali
- Limitazione dei diritti
- Discriminazione
- Furto o usurpazione di identità
- Perdite finanziarie
- Decifratura non autorizzata della pseudonimizzazione
- Pregiudizio alla reputazione
- Perdita di riservatezza dei dati protetti da segreto professionale
- Qualsiasi altro danno economico o sociale significativo

Per questo motivo è necessario gestire adeguatamente il data breach come di seguito indicato.

GESTIONE DELLA VIOLAZIONE DEI DATI PERSONALI

Le violazioni di dati personali sono gestite dal Titolare del trattamento o da un suo delegato o dalla persona designata con tale specifico compito, sotto la supervisione del RPD il quale deve essere coinvolto tempestivamente. Per gestire correttamente una violazione dei dati personali è necessario seguire i seguenti step:

Step 1: Rilevamento: identificazione e indagine preliminare
Step 2: Contenimento
Step 3: Valutazione del rischio
Step 4: Eventuale notifica all'Autorità Garante
Step 5: Eventuale comunicazione agli interessati
Step 6: Documentazione della violazione
Step 7: Verifica e revisione degli eventi



Step 1: Rilevamento: identificazione e indagine preliminare

- Chiunque rilevi che si sia verificato un caso di data breach deve immediatamente

1) **Informare**, di persona o per telefono o con mail/pec,

   a) il titolare nella persona del legale rappresentante o un suo delegato
   b) la persona designata per la procedura di data breach
   c) l'Amministratore di Sistema o un suo delegato in caso o la persona designata per la gestione del sistema informatico, nel caso in cui si tratti di violazione di dati contenuti in un sistema informatico.
   d) il Responsabile della protezione dei dati (RPD)

In caso di concreta, sospetta e/o avvenuta violazione dei dati personali, è di estrema importanza assicurare che la procedura sia affrontata **immediatamente** e **correttamente** al fine di minimizzare l'impatto della violazione e prevenire che si ripeta.

- Ricevuta la notizia dell'evento il **titolare** e/o **la persona designata** per la procedura di data breach devono immediatamente

1. **acquisire tutte le informazioni** relative all'evento (cosa è successo ? a che ora ? chi lo ha rilevato? quali elementi consentono di fornire la prova di ciò che è successo ? ecc.).

2. **compilare la scheda di rilevamento** della violazione (allegato A) che permetterà al Titolare del trattamento o al suo delegato, di condurre una valutazione iniziale riguardante la notizia dell'incidente occorso, al fine di stabilire se si sia effettivamente verificata un'ipotesi di Data Breach (violazione) e se sia necessaria un'indagine più approfondita dell'accaduto, procedendo con gli step successivi

3. **annotare l'evento nel registro** dei data breach indicandone:

   a. la data
   b. l'ora
   c. la data e l'ora in cui si è venuti a conoscenza dell'evento
   d. la fonte dalla quale si è avuta conoscenza dell'evento (ad esempio il soggetto che ne è venuto a conoscenza per primo)
   e. la descrizione della natura della violazione dei dati personali
   f. l'indicazione, ove possibile, delle categorie e del numero approssimativo di interessati coinvolti dall'evento;

g. l'indicare, ove possibile, delle categorie e del numero approssimativo di registrazioni dei dati personali coinvolti dall'evento;
h. la descrizione delle probabili conseguenze della violazione dei dati personali;
i. l'indicazione se la violazione è collegata con altre che riguardino il medesimo tipo di dati personali che siano stati violati nel medesimo modo e in un lasso di tempo relativamente breve.
j. la descrizione di eventuali azioni già poste in essere per rimediare alla violazione.

E' importante NON commettere alcuni errori:

- ✓ NON cancellare file, cartelle, messaggi, documenti, ecc. prima che siano compiuti e completati tutti gli accertamenti
- ✓ raccogliere e conservare tutte le prove, sia su carta sia digitali, di tutti gli eventi, anche di quelli che non sono stati notificati al Garante.
- ✓ NON commettere un data breach al fine di indagare su un data breach (ad esempio: non accedere abusivamente a PC o account per i quali non si è autorizzati)

Step 2: Contenimento della violazione

Una volta stabilito che un Data Breach è avvenuto, il **Titolare del trattamento**, in persona del legale rappresentante, **o un suo delegato**, consultando il RPD, dovrà **stabilire** in tempi molto brevi:

- **se esistono azioni che possano**

a) **rimuovere le cause che hanno determinato il data breach;**
b) **attenuare gli effetti negativi e limitare i danni** che la violazione potrebbe causare (ad esempio:
  - riparazione fisica di PC, server o altri strumenti utilizzati;
  - utilizzo dei file di back up per recuperare dati persi o danneggiati;
  - utilizzo temporaneo dei dati contenuti negli archivi cartacei al fine di consentire la regolare erogazione dei servizi;
  - isolamento/chiusura di un settore compromesso della rete;
  - cambio delle password di accesso;
  - aggiornamento e/o sostituzione di software o applicativi;
  - comunicazione tempestiva di istruzioni agli interessati sulle operazioni da compiere per evitare danni;
c) **ripristinare la normale operatività dei sistemi;**
d) **attivare procedure di "*escalation*"** comunicando agli organi o enti superiori, competenti, eventuali cambiamenti radicali che è necessario realizzare per risolvere le criticità rilevate;
e) **identificare le misure per evitare che lo stesso data breach possa verificarsi di nuovo**.

- **e procedere, quindi a**

  f) **comunicare tali azioni alla persona designata** per la gestione del data breach o, in alternativa, **stabilire** quali siano eventuali **altri soggetti che devono agire per contenere** la violazione;

Step 3: Valutazione del rischio

Dopo aver effettuato tali azioni, il **Titolare del trattamento**, in persona del legale rappresentante, **o un suo delegato**, consultando del RPD, dovrà **valutare il rischio** al fine di **stabilire se sia necessario notificare la violazione all'Autorità Garante** per la protezione dei dati personali.

La notifica al Garante deve essere effettuata necessariamente qualora sia **probabile** che la violazione presenti **un rischio** per i diritti e le libertà delle persone fisiche, come di seguito specificato:

VALUTAZIONE DELLA PROBABILITA' DEL RISCHIO	
se è PROBABILE che la violazione dei dati presenti un rischio per i diritti e le libertà delle persone fisiche	**se è IMPROBABILE** che la violazione comporti un RISCHIO per i diritti e le libertà delle persone fisiche
la Notifica al Garante è **OBBLIGATORIA**	- Non è necessario notificare la violazione - ma **bisogna MOTIVARE bene** la scelta - la Notifica può comunque essere effettuata anche in via **facoltativa**

Al fine di effettuare la **VALUTAZIONE SULLA PROBABILITA' DEL RISCHIO** il Titolare del trattamento o il suo delegato, consultando il RPD, valuteranno la gravità della violazione utilizzando i seguenti criteri:

FATTORI DA CONSIDERARE NELLA VALUTAZIONE DEL RISCHIO	
Tipo di violazione	Il tipo di violazione ✓ della riservatezza, ✓ della disponibilità ✓ dell'integrità va esaminato in relazione al tipo di dati e alle categorie di interessati. Rileva la circostanza che vi sia contemporaneamente una combinazione di più violazioni o una loro reiterazione.
Natura e carattere sensibile dei dati personali violati	✓ dati comuni ✓ categorie particolari di dati ✓ dati giudiziari penali

Volume dei dati violati	Più sono i dati violati maggiore è il rischio
Numero di persone fisiche interessate	Maggiore è il numero di interessati, maggiore è l'impatto che il data breach può avere
Facilità di identificazione delle persone fisiche	Si considera la maggiore o minore facilità con cui un soggetto che può accedere a dati personali compromessi riesce ad identificare persone fisiche specifiche anche abbinando i dati con altre informazioni
Gravità delle conseguenze	A seconda della natura dei dati coinvolti, il danno che potrebbe derivarne agli interessati può essere particolarmente grave: es. furto d'identità, danni fisici, danni alla reputazione , ecc.
Caratteristiche particolari dell'interessato	Se la violazione riguarda dati riferiti a Minori o altre categorie di persone vulnerabili il rischio di danno è più elevato
Caratteristiche particolari del Titolare del trattamento e natura dell'attività svolta	È importante distinguere i trattamenti effettuati per ✓ adempiere un obbligo legale o nell'esercizio di pubblici poteri ✓ erogazione di servizi pubblici essenziali ✓ erogazione di servizi facoltativi non essenziali

Quindi, saranno tempestivamente notificate le violazioni di dati personali che possono avere **effetti avversi significativi sugli individui, causando danni fisici, materiali o immateriali**, come includere, ad esempio, la perdita del controllo sui propri dati personali, la limitazione di alcuni diritti, la discriminazione, il furto d'identità o il rischio di frode, la perdita di riservatezza dei dati personali protetti dal segreto professionale, una perdita finanziaria, un danno alla reputazione e qualsiasi altro significativo svantaggio economico o sociale.

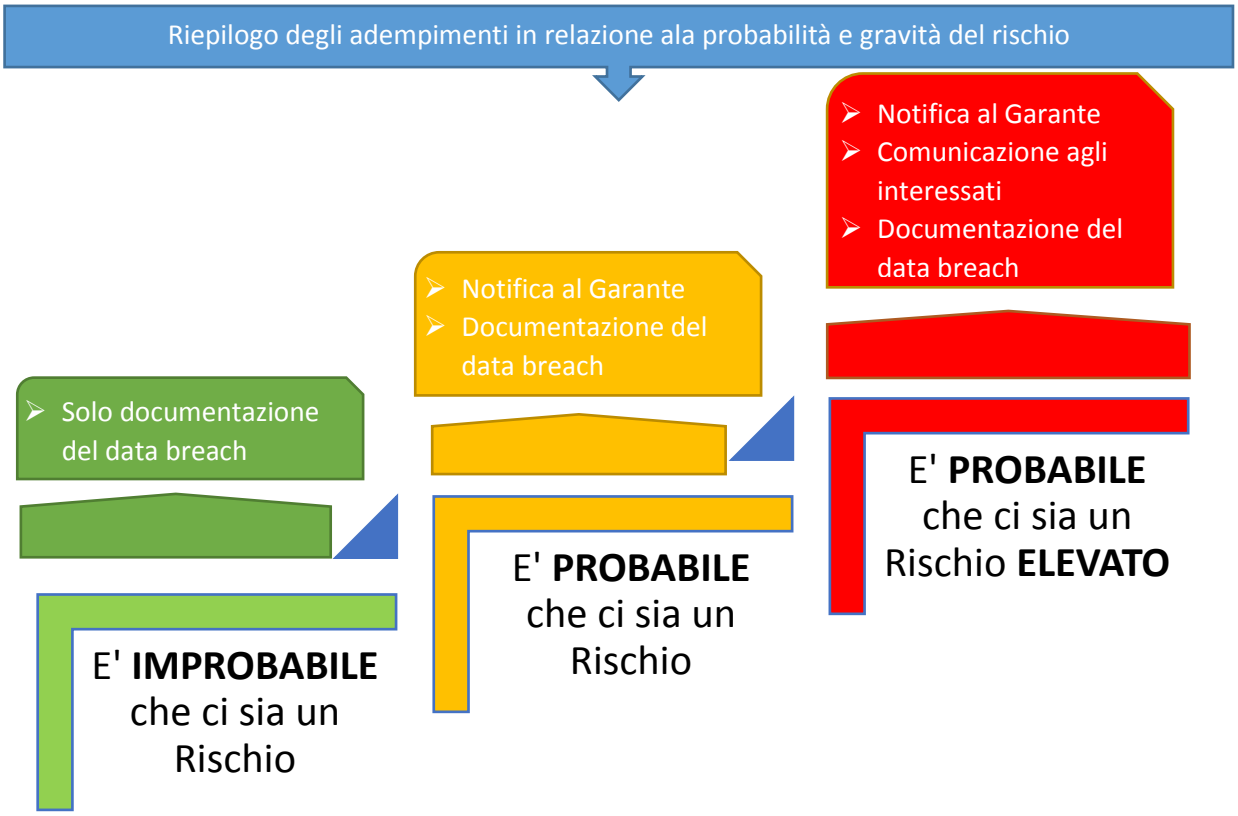
Per **VALUTARE SE IL RISCHIO E' ELEVATO** si utilizzeranno i dati e le informazioni riportati nella scheda di rilevamento -allegato A)- unitamente agli **altri elementi di valutazione successivamente acquisti** e, al fine di effettuare una stima oggettiva, corretta e motivata, si applicheranno **i** criteri sopra descritti riportati nell'allegato B - *GRIGLIA PER STIMARE LA PROBABILITA' E LA GRAVITA' DEL RISCHIO CONNESSO AL DATA BREACH,* tenendo, altresì, in debita considerazione i suggerimenti del RPD ed principi e le indicazioni previsti dall'art. 33 Del Reg. Ue n. 679/2016.

Se all'esito di tale valutazione il RISCHIO è considerato **ELEVATO**, bisognerà **verificare se è soddisfatta almeno una delle seguenti condizioni**:

a) sono state messe 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, come, ad esempio, la **cifratura** ?

b) sono state adottate subito misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati ?

In caso di risposta affermativa ad almeno una delle suddette condizioni, **non è necessario comunicare** la violazione all'interessato.



Step 4: Eventuale notifica all'Autorità Garante competente

Se all'esito dello step precedente è stata valutata la necessità di effettuare notifica della violazione dei dati subita, il Titolare, nella persona del legale rappresentante pro tempore o un suo delegato, dovrà provvedervi, **senza ingiustificato ritardo**, ove possibile entro 72 ore dal momento in cui si è avuta conoscenza dell'evento.

Se la notifica viene effettuata **oltre il termine delle 72 ore** deve essere accompagnata dai **motivi del ritardo.**

La notifica deve contenere le informazioni previste all'art. 33, par. 3 del Regolamento (UE) 2016/679 e indicate nell'allegato al Provvedimento del Garante del 30 luglio 2019 sulla notifica delle violazioni dei dati personali (doc. web n. 9126951) Tale modulo è già stato consegnato alla persona designata con lo specifico compito di gestire la presente procedura ed è, comunque, reperibile nel sito web del garante al seguente link

https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9128501

La notifica **non deve includere i dati personali oggetto di violazione** (es. non fornire i nomi dei soggetti interessati dalla violazione).

In attesa che il Garante renda prossimamente disponibile una procedura online, la notifica deve essere inviata al Garante **tramite posta elettronica certificata** all'indirizzo protocollo@pec.gpdp.it oppure tramite **posta elettronica ordinaria** all'indirizzo protocollo@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**.**

L'oggetto del messaggio deve contenere obbligatoriamente la dicitura "**NOTIFICA VIOLAZIONE DATI PERSONALI**" e opzionalmente la denominazione del titolare del trattamento.

NOTIFICA PER FASI: Se entro le 72 ore non si dispone ancora di tutte le informazioni relative all'evento, si procederà ugualmente alla notifica specificando nel modulo che si tratta di notifica ***PRELIMINARE*** che viene effettuata pur in assenza di un quadro completo.

Successivamente, dovrà essere effettuata tempestivamente una **successiva notifica integrativa** con le ulteriori informazioni che nel frattempo sono state reperite.

Step 5: Eventuale comunicazione agli interessati

Se all'esito dello step 2 è stato valutato che il **rischio è elevato** e i dati non sono stati resi incomprensibili attraverso tecniche adeguate come ad esempio la cifratura, è necessario **effettuare,** a cura del Titolare o di un suo delegato, o della persona designata con lo specifico compito di gestire la presente procedura, la **comunicazione della violazione dei dati a coloro dei cui dati si tratta**, senza ingiustificato ritardo.

Tale comunicazione deve essere chiara, trasparente, tempestiva.

Essa deve essere distinta da altre comunicazioni (quali newsletter, aggiornamenti regolari, messaggi standard), per cui bisognerà privilegiare la modalità di comunicazione diretta con i soggetti interessati (quali e-mail, SMS, messaggi diretti).

La **comunicazione deve contenere le seguenti informazioni**:

- comunicare il nome e i dati di contatto del Responsabile della protezione dei dati (RPD);
- descrivere la natura della violazione
- 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
- descrivere le misure adottate o di cui si propone l'adozione per attenuarne i possibili effetti negativi per gli interessati, fornendo indicazioni pratiche su come proteggersi dalla violazione.

Se la segnalazione diretta richiede uno **sforzo ritenuto sproporzionato**, allora si utilizzerà una **COMUNICAZIONE PUBBLICA**, effettuata tramite pubblicazione di un avviso nel sito web istituzionale, eventualmente anche sotto forma di banner o pubblicazione nei social o sulla stampa, che dovrà essere ugualmente chiaro, tempestivo ed efficace nell'informare gli interessati.

Non dovrà essere mai utilizzato un canale di contatto compromesso dalla violazione (ad esempio posta elettronica ordinaria o certificata oggetto di attacco) in quanto tale canale potrebbe essere utilizzato anche da autori di attacchi che si fanno passare per il Titolare del trattamento.

Step 6: Documentazione della violazione

Indipendentemente dalla valutazione circa la necessità di procedere a notificazione e/o comunicazione della violazione di Data Breach, ogni qualvolta si verifichi un incidente la persona designata con lo specifico compito di gestire la presente procedura, dovrà documentarlo utilizzando gli Allegati A e B, conservando ogni eventuale documento o file che possa comprovare quanto è avvenuto, registrando l'evento nel **Registro dei data breach,** che è stato predisposto.

Il report delle annotazioni effettuate dovrà essere stampato e conservato.

Tali adempimenti saranno curati dalla persona designata con il compito specifico di gestire la presente procedura con l'ausilio dell'Amministratore di sistema (qualora la violazione riguardi dati contenuti in sistemi informatici), con la consulenza e sotto la sorveglianza del RPD

Il report delle annotazioni effettuate dovrà essere trasmesso immediatamente al RPD.

Il Registro dei Data Breach deve essere continuamente aggiornato e messo a disposizione del Garante qualora l'Autorità chieda di accedervi.

Step 6: verifica e revisione degli eventi

Periodicamente il Titolare o un suo delegato, avvalendosi dei Responsabili di settore e della consulenza del RPD, effettua un'analisi finalizzata a

- scoprire eventuali violazioni che siano **rimaste nascoste**;
- individuare le **cause** delle violazioni;
- individuare i **rimedi** in relazione alle specifiche cause;
- individuare gli **effetti** che le violazioni possono avere con specifico riguardo ai diritti e alle libertà degli interessati;
- individuare le misure da mettere in atto per **prevenire e ostacolare simili violazion**i che potrebbero avvenire in futuro.

Caltanissetta lì _____

Il Titolare del Trattamento

Pres. Geom. Salvatore Tomasella

Allegato A)

SCHEDA DI RILEVAMENTO DI UNA VIOLAZIONE DELLA SICUREZZA DEI DATI PERSONALI

(DATA BREACH)

1	**Data** dell' evento	☐ Il _____ ☐ Dal _____ (la violazione è ancora in corso) ☐ Dal _____ al _____ ☐ In un tempo non ancora determinato
2	**data e ora** in cui si è venuti a **conoscenza** dell'evento	Data:_____ Ora:_____
3	data e ora del **termine di scadenza** della **notifica** al Garante (*calcolare **72 ore** dal momento in cui si è avuta conoscenza*)	Data:_____ Ora:_____
4	**Data, ora e modalità** in cui è stato **informato il RPD**	Data:_____ Ora:_____ Modalità: _____
5	**Data, ora e modalità** in cui è stato **informato il Titolare**	Data:_____ Ora:_____ Modalità: _____

6	**Indicare se è stata data comunicazione del Data Breach ad altri soggetti** *(ad esempio, ai Contitolari, ad altri Titolari, a Responsabili esterni)*	☐ **NO** ☐ **Si - indicare** Data:_____ Ora:_____ Modalità: _____
7	**fonte** attraverso la quale si è avuta conoscenza dell'evento *(eventuali **generalità complete** e **dati di contatto** (telefono, mail) della persona che per prima ha rilevato la violazione - in caso di soggetti esterni/società indicare la*	
8	**Luogo della violazione** *(indicare l'ufficio o gli uffici coinvolti)*	
9	**Dispositivi oggetto del Data Breach**	☐ computer ☐ server ☐ rete ☐ portatile ☐ tablet, smatphone ☐ chiavette usb, dispositivi di archiviazione esterne ☐ file o parte di un file ☐ account posta elettronica ☐ account PEC ☐ piattaforme on line ☐ strumento di back up ☐ documento cartaceo
10	**Se è coinvolto uno strumento di back up indicare quando è stato fatto l'ultimo back up**	☐ ultimo back up effettuato In data _____

11	**Se un laptop è stato perso/rubato: quando è stata l'ultima volta in cui il laptop è stato sincronizzato con il sistema IT centrale?**	☐ ultima sincronizzazione effettuata In data _____
12	**Soggetti interni il cui trattamento è coinvolto dall'evento**	
13	**Ulteriori soggetti esterno, il cui trattamento è coinvolto dall'evento** *(in caso di società indicare la ragione sociale - Indicare il **ruolo** svolto: contitolare, responsabile, altro titolare esterno)*	Denominazione:_____ C.f. / P.Iva: _____ Ruolo: ☐ Contitolare ☐ Responsabile esterno ☐ altro titolare per conto del quale l'ente tratta dati
14	**natura della violazione** dei dati personali *(descrivere il tipo di violazione, specificando le modalità ed eventuali nomi di soggetti coinvolti in maniera lecita o illecita, volontaria o involontaria o accidentale, denominazione dell'archivio o della banca dati coinvolto)*	☐ Perdita di confidenzialità ☐ Perdita di integrità ☐ Perdita di disponibilità
		☐ attività lecite ☐ attività illecite ☐ Attività volontarie ☐ Attività involontarie ☐ Attività accidentali
		☐ eventuali nomi di soggetti coinvolti: _____ ☐ Archivio o banca dati coinvolta: _____ ☐ Descrizione delle modalità con le quali si è verificato l'evento: _____

15	**Causa della violazione**	☐ Azione intenzionale interna ☐ Azione accidentale interna ☐ Azione intenzionale esterna ☐ Azione accidentale esterna ☐ Sconosciuta ☐ Altro (specificare): _____
16	**categorie di dati** coinvolti dall'evento	☐ Dati anagrafici (nome, cognome, sesso, data di nascita, luogo di nascita, codice fiscale, altro...) ☐ Dati di contatto (indirizzo postale o di posta elettronica, numero di telefono fisso o mobile) ☐ Dati di accesso e di identificazione (username, password, customer ID, altro…) ☐ Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro…) ☐ Dati relativi alla fornitura di un servizio di comunicazione elettronica (dati di traffico, dati relativi alla navigazione internet, altro…) ☐ Dati relativi a condanne penali e ai reati o a connesse misure di sicurezza o di prevenzione ☐ Dati di profilazione ☐ Dati relativi a documenti di identificazione/riconoscimento (carta di identità, passaporto, patente, CNS, altro…) ☐ Dati di localizzazione ☐ Dati che rivelino l'origine razziale o etnica ☐ Dati che rivelino opinioni politiche ☐ Dati che rivelino convinzioni religiose o filosofiche ☐ Dati che rivelino l'appartenenza sindacale ☐ Dati relativi alla vita sessuale o all'orientamento sessuale ☐ Dati relativi alla salute ☐ Dati genetici
17	**Volume dei dati personali coinvolti** *(stimare anche in modo approssimativo la quantità dei dati personali coinvolti dall'evento)*	☐ N._____ interessati ☐ Circa n. _____interessati ☐ Un numero ancora sconosciuto di interessati

18	**categorie di interessati** coinvolti dall'evento	☐ Dipendenti ☐ Consulenti ☐ Utenti ☐ Contraenti ☐ Abbonati ☐ Clienti (attuali o potenziali) ☐ Associati, soci, aderenti, simpatizzanti, sostenitori ☐ Soggetti che ricoprono cariche sociali ☐ Beneficiari o assistiti ☐ Pazienti ☐ Minori ☐ Persone vulnerabili (es. vittime di violenze o abusi, rifugiati, richiedenti asilo) ☐ Categorie ancora non determinate ☐ Altro (specificare) _____
19	**numero** di **interessati** (*anche approssimativo*)	☐ N._____ interessati ☐ Circa n. _____interessati ☐ Un numero (ancora) sconosciuto di interessati
20	**Descrizione dell'incidente di sicurezza alla base della violazione**	
21	**categorie** di **registrazioni** dei dati personali coinvolti	
22	**numero** approssimativo di **registrazioni** dei dati personali convolte	

23	Descrizione dei sistemi e delle infrastrutture IT coinvolti, con indicazione della loro ubicazione.	
24	Misure di sicurezza tecniche e organizzative adottate per garantire la sicurezza dei dati, dei sistemi e delle infrastrutture IT coinvolti	
25	Descrizione delle probabili **conseguenze** della violazione	**In caso di perdita di confidenzialità:** ☐ I dati sono stati divulgati al di fuori di quanto previsto dall'informativa ovvero dalla disciplina di riferimento ☐ I dati possono essere correlati, senza sforzo irragionevole, ad altre informazioni relative agli interessati ☐ I dati possono essere utilizzati per finalità diverse da quelle previste oppure in modo non lecito ☐ Altro (specificare): _____
		In caso di perdita di integrità: ☐ I dati sono stati modificati e resi inconsistenti ☐ I dati sono stati modificati mantenendo la consistenza ☐ Altro (specificare):_____
		In caso di perdita di disponibilità: ☐ Mancato accesso a servizi ☐ Malfunzionamento e difficoltà nell'utilizzo di servizi ☐ Altro (specificare): _____
		Ulteriori considerazioni sulle possibili conseguenze:_____

26	**Potenziali effetti negativi** per gli interessati	☐ Perdita del controllo dei dati personali ☐ Limitazione dei diritti ☐ Discriminazione ☐ Furto o usurpazione d'identità ☐ Frodi ☐ Perdite finanziarie ☐ Decifratura non autorizzata della pseudonimizzazione ☐ Pregiudizio alla reputazione ☐ Perdita di riservatezza dei dati personali protetti da segreto professionale ☐ Conoscenza da parte di terzi non autorizzati ☐ Qualsiasi altro danno economico o sociale significativo (specificare)
27	Modalità di esposizione al rischio	☐ lettura (presumibilmente i dati non sono stati copiati), ☐ copia (i dati sono ancora presenti sui sistemi del titolare), ☐ alterazione (i dati sono presenti sui sistemi ma sono stati alterati), ☐ cancellazione (i dati non sono più presenti e non li ha neppure l'autore della violazione), ☐ furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione)
28	Ruolo del Titolare e natura dell'attività svolta	trattamenti effettuati per ☐ adempiere un obbligo legale o nell'esercizio di pubblici poteri ☐ erogazione di servizi pubblici essenziali ☐ erogazione di servizi facoltativi non essenziali
29	La violazione può avere conseguenze negative in uno dei seguenti ambiti ?	☐ gestione dei servizi resi all'utenza ☐ ricerca ☐ finanziario, patrimoniale, contabile ☐ giudiziario ☐ responsabilità ☐ reputazione - immagine
30	La violazione concerne informazioni che possono essere utilizzate per commettere furti d'identità ?	☐ dati di accesso e di identificazione ☐ codice fiscale ☐ copie di carta d'identità ☐ passaporto ☐ carte di credito
31	La violazione coinvolge informazioni relative a performance lavorative che potrebbero causare danni significativi alle persone	☐ salario o stipendio ☐ stato di famiglia ☐ sanzioni disciplinari ☐ altro _____

32	Gli interessati rischiano di essere privati del controllo sui dati personali che li riguardano?	☐ Si ☐ No
33	Facilità con cui un soggetto che può accedere a dati personali compromessi riesce ad identificare persone fisiche specifiche anche abbinando i dati con altre informazioni	☐ Molto facile (non occorre una ricerca speciale per risalire all'identità) ☐ difficile, ma non impossibile in presenza di certe condizioni ☐ estremamente difficile
34	E' **PROBABILE** che vi sia un **RISCHIO** per i diritti e le libertà delle persone fisiche? (***MOTIVARE*** *adeguatamente*)	☐ Si ☐ No Motivazione:
35	**Misure** tecniche e organizzative adottate o di cui si propone l'adozione per porre **rimedio** alla violazione dei dati e **ridurne** gli effetti negativi per gli interessati. *(ad esempio: La pseudonimizzazione e la cifratura dei dati personali)*	
	Misure tecniche e organizzative adottate o di cui si propone l'adozione per **prevenire simili violazion**i future	
36	La violazione è suscettibile di presentare un **RISCHIO ELEVATO** per i diritti e le libertà delle persone fisiche ? (***MOTIVARE*** *adeguatamente)*	☐ Si ☐ No Motivazione:
37	**Classificazione della gravità della violazione e motivazioni:**	☐ Trascurabile ☐ Basso ☐ Medio ☐ Alto Motivazione:

38	**Prima della violazione** il titolare aveva 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 ? (ad es. cifratura)	☐ No ☐ Si, (specificare quali_____
39	Sono state **successivamente** adottate misure atte a **scongiurare il sopraggiungere** di un rischio elevato per i diritti e le libertà degli interessati ?	☐ No ☐ Si, (specificare quali_____
40	**La comunicazione** agli interessati richiederebbe **sforzi sproporzionati** (**MOTIVARE** adeguatamente)	☐ No ☐ Si, (specificare per quale motivo): _____
26	Indicare se la violazione è **collegata** con altre che riguardino il medesimo tipo di dati personali che siano stati violati nel medesimo modo e in un lasso di tempo relativamente breve.	
27	Indicare eventuali **altri documenti utili** per documentare l'evento	

Data _____ F.to Il designato per la procedura di data breach

_____

Data _____ Il Titolare - F.to Il legale rappresentante

_____

Allegato B)

GRIGLIA PER STIMARE LA PROBABILITA' E LA GRAVITA' DEL RISCHIO CONNESSO AL DATA BREACH

ALLA LUCE DELLA SCHEDA DI RILEVAMENTO E DEGLI ALTRI ELEMENTI DI VALUTAZIONE ACQUISITI

CRITERI PER VALUTAZIONE LA PROBABILITA' LA GRAVITÀ DEL RISCHIO		**Motivazione**	
Fattori da considerare alla luce della Scheda allegato A)		**PROBABILITA'**	**GRAVITA'**
Tipo di violazione	violazione ✓ della riservatezza, ✓ della disponibilità ✓ dell'integrità in relazione a ➢ tipo di dati ➢ categorie di interessati. vi è contemporaneamente una combinazione di più violazioni o una loro reiterazione ?		
Natura e carattere sensibile dei dati personali violati	Qual è il grado di sensibilità dei dati coinvolti ✓ dati comuni ✓ categorie particolari di dati ✓ dati giudiziari penali		
Volume dei dati violati	Qual è il volume dei dati coinvolti ?		
Numero di persone fisiche interessate	Qual è il numero di interessati ?		
Facilità di identificazione delle persone fisiche anche abbinando i dati con altre informazioni	☐ Molto facile (non occorre una ricerca speciale per risalire all'identità) ☐ difficile, ma non impossibile in presenza di certe condizioni ☐ estremamente difficile		
Gravità delle conseguenze a seconda della natura dei dati coinvolti	Stimare i potenziali effetti negativi per gli interessati indicati nella scheda allegato A		
Caratteristiche particolari dell'interessato	la violazione riguarda dati riferiti a ▪ Minori ▪ Anziani ▪ Disabili ▪ o altre categorie di persone vulnerabili il rischio di danno è più elevato		
Caratteristiche particolari del Titolare del trattamento e natura dell'attività svolta	distinguere i trattamenti effettuati per ✓ adempiere un obbligo legale o nell'esercizio di pubblici poteri ✓ erogazione di servizi pubblici essenziali ✓ erogazione di servizi facoltativi non essenziali		
	Giudizio finale sul Rischio	☐ **PROBABILE** ☐ **IMPROBABILE**	☐ **Trascurabile** ☐ **Basso** ☐ **Medio** ☐ **Alto**