AZIENDA SPECIALE
PROMOCAMERA
CAMERA DI COMMERCIO DI SASSARI

# SISTEMA DI GESTIONE DEI DATI PERSONALI DELLA PROMOCAMERA, AZIENDA SPECIALE DELLA CAMERA DI COMMERCIO INDUSTRIA E ARTIGIANATO DI SASSARI

## Procedura di gestione dei data breach

ai sensi del Regolamento UE 679/2016

# PREMESSA

## SCOPO E CAMPO DI APPLICAZIONE

Scopo della presente procedura è descrivere le attività relative al processo di segnalazione e gestione degli incidenti di sicurezza riguardanti i trattamenti di dati personali in qualsiasi modalità svolti dalla Promocamera, Azienda Speciale della Camera di Commercio Industria e Artigianato di Sassari, nel prosieguo indicata come "Promocamera".

Tale processo regolamenta la gestione degli allarmi di sicurezza, la conduzione delle attività investigative funzionali alla individuazione di tutti gli elementi utili alla completa definizione di una violazione, l'attivazione delle strategie di contenimento o delle azioni correttive, la gestione degli adempimenti richiesti dalla normativa nei confronti del Garante per la protezione dei dati personali e degli interessati, le modalità per la tenuta di idonee registrazioni per documentare il rispetto degli obblighi imposti nel rispetto del principio di responsabilizzazione (c.d. *accountability*).

Si fa presente che ai data breach relativi ad ipotesi in cui Promocamera svolga l'attività di responsabile esterno del trattamento, ex art. 28 del GDPR, dovranno essere osservate anche le indicazioni ed istruzioni fornite dal Titolare e contenute nel documento di designazione.

La presente procedura è portata a conoscenza, anche attraverso attività di sensibilizzazione o formazione, di tutti i Dirigenti, funzionari o, comunque, referenti delle Aree/Uffici di Promocamera.

## RIFERIMENTI NORMATIVI

La presente procedura risponde ai seguenti requisiti normativi:

1. Notifica di una violazione dei dati personali all'autorità di controllo (art. 33 del GDPR);
2. Comunicazione di una violazione dei dati personali all'interessato (art. 34 del GDPR);
3. WP250rev.01, *Guidelines on Personal data breach notification under Regulation 2016/679*, adottate il 03/10/2017 e riemesse il 06/02/2018;
4. Provv. del Garante 30 luglio 2019, n. 157, *sulla notifica delle violazioni dei dati personali (data breach).*

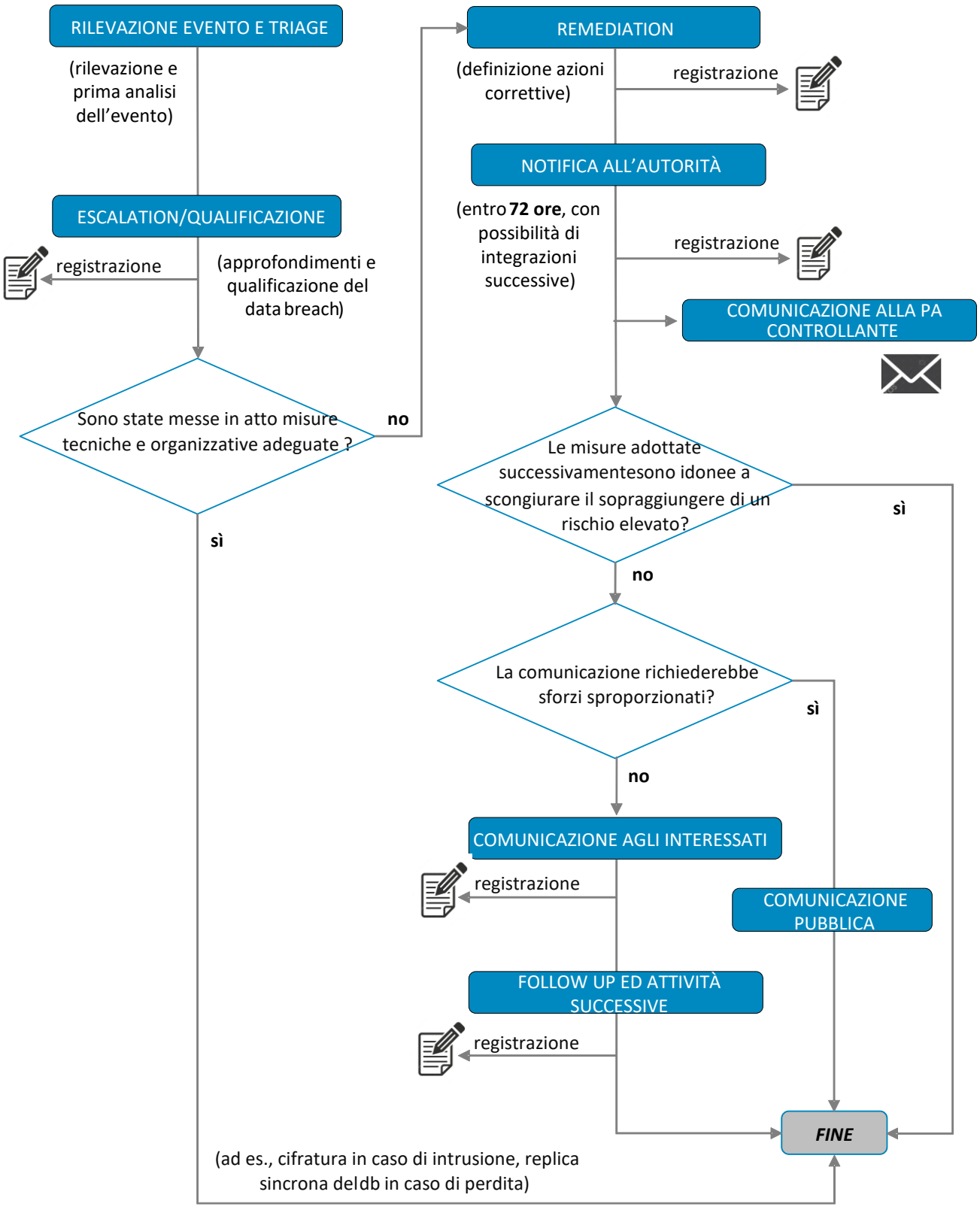
## ACRONIMI E DEFINIZIONI UTILIZZATE

| | |
|---|---|
| GDPR | Regolamento UE 2016/679 (General Data Protection Regulation) |
| Codice | D.Lgs. 196/2003 "Codice in materia di protezione dei dati personali" come modificato dal D.Lgs. 101/2018 |
| Garante | Garante per la protezione dei dati personali |
| WP29 | Working Party article 29 – Gruppo di lavoro ex art. 29 (ora Comitato europeo per la protezione dei dati) – EDPB (European Data Protection Board) |
| RPD | Responsabile della protezione dei dati |
| Delegato del Titolare | Soggetto che, secondo le deleghe/procure formalizzate ed il sistema di gestione della privacy, garantisce specifiche funzioni ai fini della *compliance* al GDPR |
| Direttore | Direttore di Promocamera |
| Evento | Qualsiasi accadimento significativo per la gestione delle infrastrutture IT e per la gestione dell'operatività dei servizi |
| Violazione (data breach) | Qualsiasi incidente di sicurezza che comporti 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 |

## MATRICE DELLA REDAZIONE E DELLE REVISIONI

| Data | Stato | Descrizione | Approvazione |
|---|---|---|---|
| 05/08/2019 | Bozza | Documento inviato via mail il 31/7/2019 | Revisioni DPO (Dott. Tripodi) |
| 02/10/2019 | Bozza | Documento inviato via mail il 26/9/2019 | Approvazione DPO (Dott. Tripodi) |
| 04/12/2019 | Testo definitivo | Approvazione documento | Delibera CdA N. 10 del 04/12/2019 |
| | | | |
| | | | |
| | | | |

La gestione di un data breach può riassumersi nelle fasi di seguito rappresentate.



## RILEVAZIONE EVENTO E TRIAGE

La rilevazione di un evento può avvenire da diverse fonti:

↘ SEGNALAZIONE AUTOMATICA: sistemi di segnalazione automatica, come le violazioni derivanti da superamento dei sistemi di Firewall interni a Promocamera.

↘ SEGNALAZIONE INTERNA: attività di monitoraggio degli eventi da parte degli amministratori di sistema; comunicazione di: malfunzionamenti irrituali o blocco dei sistemi, furti, smarrimenti, intrusioni fisiche nei locali archivio etc.

↘ SEGNALAZIONE ESTERNA: nell'ambito dell'attività di monitoraggio, assistenza e manutenzione da parte di fornitori esterni di applicativi, supporto sistemistico, servizi di consulenza, etc. ovvero da parte di utenti finali dei servizi di Promocamera.

In tutti i contratti che attribuiscano funzioni di amministrazione di sistemi o deleghino trattamenti di dati personali a soggetti esterni qualificati o qualificabili come responsabili esterni del trattamento ex art. 28 GDPR, sono presenti clausole contrattuali che prevedono l'obbligo:

- di comunicazione immediata di eventuali eventi di sicurezza che abbiano coinvolto i dati oggetto di trattamento, specificando le azioni correttive poste in atto e gli esiti delle stesse. Nello standard contrattuale è previsto che la segnalazione pervenga al Referente contrattuale di Promocamera;
- di fornire in caso di necessità, anche attraverso il RPD, la massima disponibilità e collaborazione per l'analisi e risoluzione di eventuali criticità emergenti per l'ambito di trattamento assegnato.

Le segnalazioni pervengono al Direttore o al Direttore tecnico da parte del funzionario/Ufficio coinvolto dall'evento, ovvero da parte dell'Amministratore di sistema.

Il Direttore o il Direttore tecnico provvede ad attivare (anche in modalità videoconferenza, o altre modalità di comunicazione a distanza) il Team di primo intervento (T1i) composto da:

- l'Amministratore di sistema;
- un eventuale referente delle Società in house (o esterne) coinvolte nel trattamento[1]

Il team di primo intervento, sotto la responsabilità del Direttore o del Direttore tecnico, ha il compito di verificare il perimetro dell'evento, ovvero almeno le seguenti informazioni:

1. sistema, infrastruttura, base dati oggetto dell'evento;
2. tipologia dell'evento verificatosi;
3. tipologia e volume dei dati e degli interessati coinvolti:
4. misure di sicurezza applicate;
5. attività di correttive ipotizzabili.

In caso di mancato coinvolgimento di dati personali, il Team di primo intervento attribuisce le responsabilità per l'avvio delle eventuali azioni correttive e registra l'evento su una apposita scheda di rilevazione. Ad esito delle azioni correttive, la fase si chiude con un resoconto delle evidenze riscontrate e delle attività svolte/da svolgere.

Nel caso in cui l'evento coinvolga dati personali, viene attivata una successiva fase che comporta la segnalazione della scheda di registrazione al RPD e la costituzione del Team di Secondo intervento (T2i).

**Questa fase deve concludersi entro 36 ore dalla rilevazione dell'evento.**

[1] A norma dell'art. 28, par. 3, lett. h) del GDPR, il Responsabile del trattamento "mette a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi… e consente e contribuisce alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato".

## ESCALATION, QUALIFICAZIONE DELLA VIOLAZIONE E REMEDIATION

Alla ricezione della scheda di segnalazione, il Direttore o il Direttore tecnico procede alla costituzione del Team di Secondo intervento (T2i) costituito da:

- il RPD;
- l'Amministratore di sistema;
- lo specialista della società o soggetto che ha realizzato/fornito il prodotto/servizio interessato dall'incidente
- il referente specializzato della Società in house eventualmente coinvolta nel trattamento[2]
- il Responsabile del Servizio/Capo Progetto responsabile del processo in relazione al quale si ipotizza la violazione di dati;

Il Team di Secondo intervento può, se del caso, essere integrato da:

- un referente dell'Amministrazione;
- l'eventuale consulenza tecnica o giuridica qualora necessaria.

Il Team ha il compito di verificare, a norma dell'art. 33, par. 1, del GDPR, la probabilità che la violazione dei dati personali presenti un rischio (soprattutto se questo può qualificarsi come "elevato") per i diritti e le libertà delle persone fisiche e, di conseguenza, decidere le misure di risposta all'emergenza.
A tal fine:

a) sono raccolte o consolidate/approfondite le informazioni di cui al format per la comunicazione al garante (cfr. All. 1), ove disponibili, anche al fine di minimizzare i tempi di risposta;
b) sono effettuate le seguenti valutazioni[3]:
   - natura della violazione e potenziale esposizione degli interessati (c.d. gravità dell'accadimento);
   - priorità, in funzione dell'urgenza (valutata sulla base di quanto velocemente potrebbero verificarsi danni);
   - impatto potenziale dell'esposizione degli interessati (valutazione dell'entità dei danni agli interessati)[4];
   - adeguatezza delle misure di sicurezza già implementate rispetto al potenziale danno arrecabile agli interessati.

Ad esito dell'analisi:

A. nel caso in cui la violazione – in funzione dell'adeguatezza delle misure implementate – non costituisca un rischio per gli interessati, il Direttore o il Direttore tecnico ovvero un loro delegato provvede a verbalizzare gli esiti dell'analisi riportando esplicitamente il parere formalizzato dal RPD; copia del verbale deve essere inviato:
   - al RPD che provvede, attraverso il suo staff di supporto, a far aggiornare il "Registro dei Data Breach" come da format allegato (All. 2)
   - al Direttore, in qualità di Delegato del Titolare del trattamento per la condivisione finale sull'esito delle valutazioni.
B. nel caso in cui sia stato valutato che le misure implementate siano insufficienti alla tutela degli interessati:
   1. il team provvede ad identificare le possibili azioni correttive da implementare, selezionandole tra quelle di cui sia valutata la fattibilità immediata ed il miglior esito ai fini della minimizzazione del possibile danno agli interessati;
   2. il Direttore provvede a:
      - definire ed assegnare responsabilità e tempistiche per la remediation, compresi i soggetti esterni coinvolti;
      - verbalizzare gli esiti dell'analisi riportando esplicitamente il parere formalizzato dal RPD;
      - compilare o completare il Modello per la notificazione (all. 1), indicando se le azioni correttive (c.d. attività di remediation) sono già concluse od ancora in itinere.

**<u>Questa fase deve concludersi entro ulteriori 36 ore dalla rilevazione dell'evento</u>.**

[2] Cfr. nota n. 1

[3] Per la valutazione qualitativa degli impatti è possibile partire dai parametri di gravità/probabilità utilizzati nell'ambito dell'assessment dei trattamenti dell'Ente e dai valori ivi rilevati, procedendo per successivi affinamenti fino a focalizzare l'analisi sull'asset colpito dalla violazione.

[4] Ovvero danno fisico, materiale o immateriale, in particolare: perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti; discriminazioni; furto o usurpazione d'identità; perdite finanziarie; pregiudizio alla reputazione; perdita di riservatezza dei dati personali protetti da segreto professionale; decifratura non autorizzata della pseudonimizzazione; qualsiasi altro danno economico o sociale significativo" cfr. considerando 75 e 85 GDPR

## INVIO DELLE NOTIFICAZIONI

Il Garante, con il provv. 30 luglio 2019, n. 157, ha definito il Modello per la notifica delle violazioni dei dati personali, ai sensi dell'art. 33 del GDPR e dell'art. 26 del D.Lgs. n. 51/2018. Il Modello, secondo le modalità di cui all'art. 65 del D.Lgs. n. 82/2005 (CAD), è riprodotto nell'Allegato 1 al presente documento.

La notifica avviene mediante la compilazione del Modello nell'ambito dei sistemi telematici indicati nel sito istituzionale del Garante.

Il Modello deve essere sottoscritto con firma digitale dal Direttore ed inviato formalmente al Garante nel più breve tempo possibile, possibilmente entro 72 ore dall'avvenuta conoscenza da parte del Titolare.

Ove avvenga oltre tale limite temporale è necessario corredarla dei motivi del ritardo[5].

Qualora non si disponga di tutte le informazioni previste dal format, è possibile inviare una prima notifica parziale, da completare non appena disponibili le ulteriori informazioni.

Il verbale ed il Modello sottoscritto dal Direttore è inviato:

- al RPD che provvede, attraverso il suo staff di supporto, a far aggiornare il "Registro dei Data Breach";
- al referente dell'Amministrazione Pubblica da cui eventualmente Promocamera ha ricevuto l'incarico di trattare i dati personali[6], previa valutazione di opportunità condotta congiuntamente con il Direttore ed a seguito dell'avvenuta notifica al Garante.

Ove le misure di cui al punto B) del paragrafo precedente siano adottate immediatamente, la fase si chiude con il resoconto delle evidenze riscontrate e delle attività svolte/da svolgere (mediante verbalizzazione degli esiti da parte del Dirigente dell'Area di riferimento)[7]

Nel caso in cui tali misure necessitino di maggior tempo per l'implementazione ovvero non siano in grado di minimizzare i rischi per gli interessati, il Dirigente dell'Area di riferimento:

a) provvede a definire i contenuti della comunicazione agli interessati, che – con linguaggio semplice e chiaro - deve contenere almeno i seguenti elementi:
   - la natura della violazione dei dati personali;
   - le probabili conseguenze della violazione dei dati personali;
   - le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione;
   - il nome e i dati di contatto del responsabile della protezione dei dati.

   La comunicazione è sottoposta a parere del RPD e ad approvazione del Direttore.

b) verifica la fattibilità di reperimento dei dati di contatto degli interessati coinvolti o potenzialmente coinvolti; nel caso in cui si valuti che la comunicazione agli interessati possa essere sostenuta senza sforzi sproporzionati (ad es., disponibilità di email/pec), provvede all'invio massivo della comunicazione.

c) Ove non vi sia disponibilità di dati di contatto ovvero si valuti che la comunicazione richieda sforzi sproporzionati, provvede a darne pubblicità nelle modalità concordate con Direttore e RPD (ad es., pubblicazione in evidenza sul sito istituzionale, comunicati stampa, etc.).

La comunicazione agli interessati deve essere formalizzata "senza ingiustificato ritardo".

Dell'avvenuta comunicazione è data informazione al RPD.

[5] ad es., data breach particolarmente complesso, serie di attacchi/violazioni consecutive che necessitano di una reazione complessa.
[6] Ad es., sulla base di una convenzione/protocollo d'intesa.
[7] "Non è richiesta la comunicazione all'interessato… se 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" (art. 34, par. 3, lett. b del GDPR).

## ATTIVITA' SUCCESSIVE

Se durante le fasi precedenti si sospetta che la violazione possa essere stata provocata in maniera intenzionale da un esterno o da un utente interno si attiva il processo di raccolta delle evidenze o prove con ulteriori investigazioni anche difensive.

L'attività, ove necessario, può essere gestita secondo quanto previsto dall'art. 391 nonies[8] o dall'art. 327 bis c.p.p.[9] e deve rispettare gli standard e le normative (raccolta e "catena di custodia") in termini di analisi forense al fine di poter intraprendere successivamente un'azione legale nei confronti dell'eventuale responsabile.

Qualora non si riscontrasse questa condizione, l'analisi post-violazione sarà finalizzata all'apprendimento delle cause che hanno generato l'evento al fine di imparare dai propri errori e per fornire ulteriori informazioni per la risoluzione di eventuali criticità collegate o ricorrenti.

Ad esito delle notificazioni al Garante ed agli interessati, il RPD deve:

- gestire in prima persona le relazioni e gli eventuali feedback pervenuti dal Garante e dalle altre Istituzioni coinvolte, facendo aggiornare il "Registro dei Data Breach";
- gestire le comunicazioni, istanze e richieste da parte degli Interessati, anche attraverso un referente dell'Area Amministrativa o dell'Area di riferimento per la violazione.

La compilazione e l'aggiornamento del "Registro dei Data Breach" – sotto la supervisione del RPD – è svolto dal personale di supporto al RPD.

[8] Se precedente all'instaurazione di un procedimento penale.
[9] Se già instaurato il procedimento.

## MATRICE DELLE RESPONSABILITA'

**Legenda**

- R = Responsabile
- C = Coinvolto
- I = Informato

| *Fase* | *Attività* | *Soggetto/ Struttura* | Direttore | Responsabile della Protezione dei Dati | Amministratore di sistema | Società esterne Responsabili del trattamento | |
|---|---|---|---|---|---|---|---|
| ***RILEVAZIONE E TRIAGE*** | Rilevazione evento | | **R** | | **C** | **C** | |
| | Triage | | **R** | | **R** | **R** | |
| | Escalation | | **R** | **I** | **I** | **I** | |
| | | | | | | | |
| ***QUALIFICAZIONE*** | Raccolta informazioni | | **R** | **C** | **C** | **C** | |
| | Valutazione d'impatto | | **R** | **C** | **C** | **C** | |
| | Verbalizzazione esiti | | **R** | **I** | | | |
| | Tracciamento su Registro Data Breach | | | **R** | | | |
| | Identificazione azioni correttive | | **R** | **C** | | | |
| | Implementazione azioni correttive | | **R** | | **R** | **R** | |
| | Compilazione format notifica | | **R** | **C** | | | |
| | Monitoraggio azioni correttive | | **R** | **C** | **C** | **C** | |
| | | | | | | | |
| ***NOTIFICAZIONI*** | Sottoscrizione ed invio format notifica | | **R** | **C** | | | |
| | Informativa a PA partner | | **R** | | | | |
| | Predisposizione comunicazione Interessati | | **C** | **C** | | | |
| | Approvazione comunicazione | | **R** | **C** | | | |
| | Invio o pubblicazione comunicazione | | **R** | **I** | | | |
| | | | | | | | |
| ***ATTIVITÀ SUCCESSIVE*** | Avvio indagini difensive | | **R** | **I** | | | |
| | Rapporti con il Garante | | **C** | **R** | | | |
| | Rapporti con Interessati | | **R** | **C** | | | |
| | | | | | | | |

## ALLEGATO 1 – MODELLO DI NOTIFICA AL GARANTE

**Si allega il modello PDF di cui al provvedimento del Garante sulla notifica delle violazioni dei dati personali (data breach) - 30 luglio 2019 [9126951]**

## ALLEGATO 2 – REGISTRO DEI DATA BREACH

| N. record/anno | Banca dati coinvolta dalla violazione | Processo/progetto ed Area di riferimento | Cause della violazione (vulnerabilità) | Tipologia e modalità di realizzazione | Azioni correttive adottate | Follow up azioni correttive | Notifica al Garante (sì/no) | Notifica agli Interessati (sì/no) | Prescrizioni specifiche del Garante |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |

## ALLEGATO 3 – CONTATTI DI EMERGENZA DEI SOGGETTI COINVOLTI NELLA PROCEDURA

| | |
|---|---|
| RPD Promocamera | Responsabile per la protezione dei Dati (RPD / DPO)<br>% Promocamera – Azienda Speciale della Camera di Commercio I.A.A. di Sassari<br>Sede operativa: Via Predda Niedda, 18<br>07100 Sassari (SS)<br>E-mail: rpd-privacy@promocamera.it<br>PEC: rpd-privacy@pec.promocamera.it |
| Amministratore di sistema | Per.Ind. Giancarlo Rosa domiciliato presso il suo studio in Sassari, via Armando Diaz, 20 – PEC giancarlo.rosa@pec.aruba.it – Email ads@giancarlorosa.it |
| Direttore | Dott. Pietro Esposito<br>% Promocamera – Azienda Speciale della Camera di Commercio I.A.A. di Sassari<br>Sede operativa: Via Predda Niedda, 18<br>07100 Sassari (SS)<br>E-mail: protocollo@promocamera.it<br>PEC: protocollo@pec.promocamera.it |
| | |
| | |
| | |
| | |

## ALLEGATO 4 – MODELLO DI COMUNICAZIONE ALL'INTERESSATO (*)

| | |
|---|---|
| **Denominazione del Titolare del trattamento** | Promocamera – Azienda Speciale della Camera di Commercio I.A.A. di Sassari<br>Sede operativa: Via Predda Niedda, 18<br>07100 Sassari (SS) |
| Dati di contatto | E-mail: protocollo@promocamera.it<br>PEC: protocollo@pec.promocamera.it |
| **Soggetto che effettua la notifica** | |
| Ruolo del soggetto che effettua la notifica | |
| **Responsabile della Protezione dei dati** | Responsabile per la protezione dei Dati (RPD / DPO)<br>% Promocamera – Azienda Speciale della Camera di Commercio I.A.A. di Sassari<br>Sede operativa: Via Predda Niedda, 18<br>07100 Sassari (SS) |
| Dati di contatto del RPD | E-mail: rpd-privacy@promocamera.it<br>PEC: rpd-privacy@pec.promocamera.it |
| | |
| | |

| | |
|---|---|
| **Interessato destinatario della comunicazione** | |

| Modalità della comunicazione |
|---|
| ☐ Raccomandata A/R<br>☐ PEC<br>☐ Posta elettronica<br>☐ Fax<br>☐ Altro: _____ |

Spett. Società/Egr. Sig……./

siamo spiacenti di informare che in data …….. abbiamo rilevato di aver subito una violazione dei dati personali la riguardano.

(*) Qualora la comunicazione richieda – ex art. 34, par. 3, lett. c) del GDPR – uno sforzo proporzionato (in relazione, per es. alle attività da svolgere e/o ai costi da sostenere), "(…) si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia".

Nel prosieguo, in termini sintetici, è fornito – ai sensi di quanto previsto dall'art. 34 Regolamento UE n. 679/2016 (GDPR) – un quadro di quanto è accaduto.

La violazione è stata anche notificata al Garante.

Breve descrizione della violazione di dati personali e delle sue modalità

Dispositivo oggetto della violazione

☐ Computer

☐ Dispositivo mobile

☐ Documento cartaceo

☐ File o parte di un file

☐ Strumento di back-up

☐ Rete

☐ Altro:

Tipologia di dati coinvolti nella violazione

☐ Dati anagrafici

☐ Numero di telefono (fisso o mobile)

☐ Indirizzo di posta elettronica

☐ Dati di accesso e di identificazione (user name, password, customer ID, altro)

☐ Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro)

☐ Altri dati di personali (sesso, data di nascita, età, ...), dati particolari, sanitari e giudiziari

☐ Ancora sconosciuto

☐ Altro:

Tipo di violazione

☐ 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 sui sistemi del titolare 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)

☐ Altro:

Livello di gravità della violazione dei dati personali e possibili conseguenze

Indicare:

A) Numero approssimativo di registrazioni dei dati personali oggetto della violazione
B) Categoria e numero approssimativo degli interessati coinvolti dalla violazione
C) Livello di gravità elevato della violazione per i diritti e le libertà delle persone fisiche
D) Possibili conseguenze della violazione.

*(secondo le valutazioni del Titolare)*

Misure tecniche e organizzative applicate preventivamente e quelle applicate successivamente alla violazione per porre rimedio alla violazione o per attenuarne le conseguenze