

**Comune di Calcinaia**  
**Servizio Segreteria e Affari Generali**

**PROCEDURA DI GESTIONE DELLE  
VIOLAZIONI DI DATI PERSONALI  
“DATA BREACH”  
)**

**Comune di Calcinaia**  
**Servizio Segreteria e Affari Generali**

**Sommario**

I.	INTRODUZIONE.....	1
1		
A.	SCOPO.....	1
B.	CAMPO DI APPLICAZIONE.....	1
C.	DEFINIZIONE DI DATA BREACH.....	1
D.	NORMATIVA DI RIFERIMENTO.....	1
II.	RESPONSABILITÀ/AUTORITÀ E SOGGETTI COINVOLTI.....	3
III.	DESCRIZIONE DEL PROCESSO “DATA BREACH” PRESSO L’ENTE IN QUALITÀ DI TITOLARE....	3
A.	FASE 1: RACCOLTA DELLE INFORMAZIONI.....	3
1.	CANALI INTERNI .....	3
2.	CANALI ESTERNI .....	3
3.	MODALITA’ DI COMUNICAZIONE .....	3
B.	FASE 2: ANALISI DELLE SEGNALAZIONI .....	4
1.	ANALISI PRELIMINARE E ELABORAZIONE DELLA SCHEDA EVENTO.....	4
2.	ANALISI DI PRIMO LIVELLO - VERIFICA DELLA SEGNALAZIONE.....	4
3.	ANALISI DI SECONDO LIVELLO - SCHEDA VIOLAZIONE DATI.....	4
C.	FASE 3: NOTIFICA E COMUNICAZIONE .....	6
1.	NOTIFICA ALLA AUTORITÀ DI CONTROLLO.....	6
2.	COMUNICAZIONE DELLA VIOLAZIONE ALL’INTERESSATO .....	7
D.	FASE 4: REGISTRAZIONE SEGNALAZIONE NEL REGISTRO DEI “DATA BREACH” .....	7
E.	FASE 5: ANALISI POST VIOLAZIONE .....	8
IV.	DESCRIZIONE PROCESSO: “DATA BREACH” PRESSO L’ENTE O UN TERZO IN QUALITÀ DI RESPONSABILE ESTERNO.....	8
A.	OBBLIGHI DI COMUNICAZIONE DELL’ ENTE QUANDO OPERA IN QUALITÀ DI RESPONSABILE ESTERNO.....	8
B.	OBBLIGHI DI COMUNICAZIONE DI UN RESPONSABILE ESTERNO NEI CONFRONTI DELL’ENTE	8
C.	OBBLIGHI DI COMUNICAZIONE IN CASO DI CONTITOLARITA' DEL TRATTAMENTO.....	9
V.	ALLEGATI.....	11
	ALL. A SCHEDA EVENTO.....	12
	ALL. B SCHEDA VIOLAZIONE DATI.....	13
	ALL. C REGISTRO DEI DATA BREACH.....	14
	Allegato 1 MODELLO DI COMUNICAZIONE ALL’INTERESSATO DELLA VIOLAZIONE .....	15
	APPENDICE "GLOSSARIO E ACRONIMI" .....	18

# Comune di Calcinaia

## Servizio Segreteria e Affari Generali

### I. INTRODUZIONE

#### A. SCOPO

La presente procedura di gestione delle violazioni di Dati Personali ("*Data Breach*") ha lo scopo di fornire le indicazioni pratiche e di individuare gli adempimenti da eseguire in caso di violazione dei Dati Personali.

I termini riportati con lettera iniziale maiuscola, utilizzati nella presente procedura, si riferiscono alle definizioni adottate nel GDPR e riportate per comodità nell'Appendice "GLOSSARIO E ACRONIMI".

#### B. CAMPO DI APPLICAZIONE

La presente procedura si applica all'Ente **Comune di Calcinaia** in qualità di Titolare del Trattamento dei dati personali, e riguarda tutti i servizi che svolgono attività di trattamento dei dati personali nei casi in cui si verifichi una violazione o una sospetta violazione di dati personali.

#### C. DEFINIZIONE DI DATA BREACH

Per violazione di dati personali, c.d. *Data Breach*, si intende un'incidente di sicurezza che comporta accidentalmente o in modo illecito:

la **distruzione** (non esistono più i dati o non esistono più in forma che possa essere utilizzata dal Titolare), la **perdita** (il Titolare non ha più il controllo sui dati o il Titolare non ha più i dati), la **modifica** (alterazione del dato, incompletezza del dato), la **divulgazione** o l'**accesso** non autorizzato ai dati personali trasmessi, conservati o comunque trattati. Solo nel caso siano coinvolti dati personali si applica il GDPR.

Si possono distinguere tre categorie di violazioni:

- 1) Violazione della riservatezza: quando si ha una divulgazione di dati non prevista o quando accedono ai dati soggetti non autorizzati.
- 2) Violazione dell'integrità: quando il dato è alterato in modo accidentale o non autorizzato.
- 3) Violazione della disponibilità dei dati: quando accidentalmente, o per dolo, il Titolare non può accedere ai dati o questi sono stati distrutti.

Una violazione può comprendere anche tutte e tre le categorie sopra indicate o combinazioni di esse.

Quando la violazione riguarda la riservatezza del dato è facilmente individuabile, meno chiara può essere la violazione relativa alla disponibilità del dato. Ci sarà sempre una violazione della disponibilità nel caso di perdita o distruzione dei dati. L'indisponibilità dei dati è quindi da considerare una violazione quando potrebbe avere un impatto significativo sui diritti e le libertà delle persone fisiche. Non si tratta di violazione quando l'indisponibilità è dovuta a interruzioni programmate per la manutenzione.

#### D. NORMATIVA DI RIFERIMENTO

La normativa di riferimento è costituita dal "**Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati**" (di seguito GDPR) e al **D. Lgs. n. 196/2003** come emendato dal D. Lgs. 101/2018, recante "**Codice in materia di protezione dei dati personali**" (di seguito Codice)

La procedura da seguire in caso di violazione di dati personali, come sopra definita, trova specifica disciplina nei seguenti articoli del GDPR:

#### Articolo 33 - Notifica di una Violazione dei Dati Personali all'Autorità di controllo

1. 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

## Comune di Calcinaia

### Servizio Segreteria e Affari Generali

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.

2. Il Responsabile del Trattamento informa il Titolare del Trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della Violazione.
3. La notifica di cui al paragrafo 1 deve almeno:
  - a) 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;
  - b) comunicare il nome e i Dati di contatto del Responsabile della Protezione dei Dati o di altro punto di contatto presso cui ottenere più informazioni;
  - c) descrivere le probabili conseguenze della Violazione dei Dati Personali;
  - d) 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.
4. 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.
5. Il Titolare del Trattamento documenta 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 del presente articolo.

#### **Articolo 34 - Comunicazione di una Violazione dei Dati Personali all'Interessato**

1. 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.
2. La comunicazione all'Interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della Violazione dei Dati Personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d).
3. Non è richiesta la comunicazione all'Interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni:
  - a) 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;
  - b) 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 di cui al paragrafo 1;
  - c) 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.
4. Nel caso in cui il Titolare del Trattamento non abbia ancora comunicato all'Interessato la Violazione dei Dati Personali, l'Autorità di controllo può richiedere, dopo aver valutato la probabilità che la Violazione dei Dati Personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta.

## **II. RESPONSABILITÀ/AUTORITÀ E SOGGETTI COINVOLTI**

La responsabilità del seguente processo è del Titolare del Trattamento dei Dati Personali (Comune di Calcinaia) che dovrà comunicare all'Autorità di controllo e, laddove necessario e possibile, anche agli Interessati, la Violazione (*Data breach*) verificatasi.

## Comune di Calcinaia

### Servizio Segreteria e Affari Generali

In particolare, i soggetti che intervengono nel processo, in base ai diversi ruoli ricoperti, sono:

- RAPPRESENTANTE LEGALE E/O SUO DELEGATO (Sindaco o suo delegato);
- Unità di Supporto Privacy (USP) ;
- SISTEMI INFORMATIVI (IT/SECURITY);
- Responsabile Protezione Dati (di seguito RPD o anche DPO *Data Protection Officer*);
- RESPONSABILE DEL SERVIZIO OVE LA VIOLAZIONE SI È VERIFICATA (c.d. Designato Responsabile del trattamento dei dati);
- ALTRI SOGGETTI INTERNI e/o ESTERNI EVENTUALMENTE COINVOLTI NEL TRATTAMENTO (Referenti del trattamento dei dati/ Autorizzati al trattamento dei dati / Responsabili ESTERNI/eventuali CONTITOLARI).

Nelle fasi descritte di seguito sono illustrate le modalità d'intervento operativo di ciascun soggetto coinvolto.

### III. DESCRIZIONE DEL PROCESSO “DATA BREACH” PRESSO L’ENTE IN QUALITÀ DI TITOLARE.

#### A. FASE 1: RACCOLTA DELLE INFORMAZIONI

##### 1. CANALI INTERNI

Le segnalazioni interne di eventi anomali possono:

- pervenire da tutte le figure coinvolte all'interno dell'ente nel sistema di gestione *privacy* (Titolare, Designato Responsabile del trattamento dei dati/Referente del trattamento dei dati/Autorizzato al trattamento dei dati)
- pervenire da tutto il personale dell'Ente;
- essere inoltrate dal RPD.

##### 2. CANALI ESTERNI

Le segnalazioni possono pervenire anche da fonti esterne, o anche dall'analisi di informazioni presenti sul Web, ovvero dai Responsabili esterni.

Inoltre, ogni Interessato può segnalare, anche solo in caso di sospetto, che i propri Dati Personali siano stati utilizzati abusivamente o fraudolentemente da un terzo; in tal caso, l'Interessato può richiedere all'Ente la verifica dell'eventuale Violazione.

##### 3. MODALITÀ DI COMUNICAZIONE

Le segnalazioni, a qualunque soggetto/servizio/ufficio pervengano, devono essere tempestivamente comunicate al Titolare e al RPD, comunque non oltre 12/24 ore dalla conoscenza della Violazione, ai seguenti indirizzi di posta elettronica: [rpd@comune.calcinaia.pi.it](mailto:rpd@comune.calcinaia.pi.it)

#### B. FASE 2: ANALISI DELLE SEGNALAZIONI

##### 1. ANALISI PRELIMINARE E ELABORAZIONE DELLA SCHEDA EVENTO

Il Responsabile del Servizio interessato dalla potenziale violazione (c.d. Designato al trattamento dei dati), con il coinvolgimento e il supporto del RPD/DPO, avvia un'analisi preliminare finalizzata alla raccolta delle informazioni concernenti l'anomalia e alla compilazione della **Scheda Evento** (ALL. A) allegata alla presente procedura, contenente tutte le informazioni raccolte:

## Comune di Calcinaia

### Servizio Segreteria e Affari Generali

- Data evento anomalo
- Data presunta di avvenuta Violazione
- Data e ora in cui si è avuta conoscenza della Violazione
- Fonte segnalazione
- Tipologia della Violazione e di informazioni coinvolte
- Descrizione evento anomalo
- Numero Interessati coinvolti
- Numerosità di Dati Personali di cui si presume una Violazione
- Indicazione del luogo in cui è avvenuta la Violazione dei Dati, specificando la circostanza (ad esempio: smarrimento di Device Mobili, etc.)
- Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei Dati coinvolti, con indicazione della loro ubicazione.

La Scheda Evento viene, a questo punto, destinata all'analisi di primo livello descritta di seguito.

#### 2. ANALISI DI PRIMO LIVELLO - VERIFICA DELLA SEGNALAZIONE

Obiettivo dell'analisi di primo livello è quella di verificare che la segnalazione non si tratti di un cd. "falso positivo".

Nel caso in cui l'anomalia/l'incidente (Violazione dei Dati Personali) siano accertati, il Responsabile del Servizio interessato dalla potenziale violazione (Designato al trattamento dei Dati), con il coinvolgimento e il supporto del RPD e con l'eventuale collaborazione degli uffici interessati se necessario, del Servizio Informativo dell'Unione Valdera, recupera le informazioni di dettaglio sull'evento, necessarie alle analisi di secondo livello, e le riportano nella Scheda Evento (ALL. A).

Nel caso in cui l'evento segnalato risulti essere un "falso positivo", si chiude l'incidente. L'evento viene comunque inserito a cura del RPD nel "**Registro dei Data Breach**" (ALL. C), allegato alla presente procedura, nell'apposita sezione dedicata agli "eventi falsi positivi".

#### 3. ANALISI DI SECONDO LIVELLO - SCHEDA VIOLAZIONE DATI

Per l'analisi di secondo livello sono convocate e messe in contatto, tramite i diversi mezzi di comunicazione disponibili (telefono, e-mail, etc.), le seguenti strutture aziendali:

- RAPPRESENTANTE LEGALE E/O SUO DELEGATO (Sindaco o suo delegato);
- USP Unità Supporto Privacy, (composta dai membri del gruppo per la transizione digitale);
- SISTEMI INFORMATIVI
- Responsabile Protezione Dati;
- RESPONSABILE DEL SERVIZIO OVE LA VIOLAZIONE SI È VERIFICATA (c.d. Designato al trattamento dei dati);
- ALTRI SOGGETTI INTERNI e/o ESTERNI EVENTUALMENTE COINVOLTI NEL TRATTAMENTO (Referenti del trattamento dei dati/ Autorizzati al trattamento dei dati / Responsabili ESTERNI/ eventuali CONTITOLARI).

## Comune di Calcinaia

### Servizio Segreteria e Affari Generali

In tutti i casi si procede ad analizzare congiuntamente tutte le informazioni raccolte e a redigere una **Scheda Violazione Dati** (ALL. B) allegata alla presente procedura, per le conseguenti valutazioni.

Il gruppo coinvolto classifica l'evento tra i seguenti casi di violazione (inserire la sigla in corrispondenza del campo "**natura evento**" della Scheda evento):

- distruzione di Dati illecita (DDI);
- perdita di Dati illecita (PDI);
- modifica di Dati illecita (MDI);
- distruzione di Dati accidentale (DDA);
- perdita di Dati accidentale (PDA);
- modifica di Dati accidentale (MDA);
- divulgazione di Dati non autorizzata (DID);
- accesso ai Dati personali illecito (ADI).

La Violazione deve essere valutata secondo i livelli di rischio:

- **NULLO**
- **BASSO**
- **ALTO**
- **MOLTO ALTO**

Il rischio è riferito alla probabilità che si verifichi una delle seguenti condizioni a danno di persone fisiche, anche diverse dall'Interessato, a cui si riferiscono i Dati, a causa della Violazione dei Dati Personali:

1. discriminazioni
2. furto o usurpazione d'identità
3. perdite finanziarie
4. pregiudizio alla reputazione
5. perdita di riservatezza dei Dati Personali protetti da segreto professionale
6. decifrazione non autorizzata della pseudonimizzazione
7. danno economico o sociale significativo
8. privazione o limitazione di diritti o libertà
9. impedito controllo sui Dati Personali all'Interessato
10. danni fisici, materiali o immateriali alle persone fisiche.

Saranno, inoltre, valutate, come variabili qualitative dell'impatto temuto, le seguenti eventuali condizioni:

- a) che si tratti di Dati idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché di Dati genetici, Dati relativi alla salute o Dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza;
- b) che si tratti di Dati relativi a valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali;
- c) che si tratti di Dati di persone fisiche vulnerabili, in particolare minori;

## Comune di Calcinaia

### Servizio Segreteria e Affari Generali

- d) che il Trattamento riguardi una notevole quantità di Dati Personali;
- e) che il Trattamento riguardi un vasto numero di Interessati.

Il gruppo coinvolto deve provvedere affinché siano tempestivamente adottate misure che consentano di minimizzare le conseguenze negative della Violazione.

#### C. FASE 3: NOTIFICA E COMUNICAZIONE

##### 1. NOTIFICA ALLA AUTORITÀ DI CONTROLLO

Redatta la Scheda Violazione Dati (ALL. B), il gruppo deve valutare le azioni da intraprendere, avviare la notificazione verso l'Autorità di Controllo e, ove necessario, la comunicazione agli Interessati.

Il Titolare **Comune di Calcinaia**, con il coinvolgimento e con il supporto del RPD, notifica la Violazione al Garante per la Protezione dei Dati personali senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, salvo che sia improbabile che la rilevata Violazione dei Dati Personali presenti un rischio per i diritti e le libertà delle persone fisiche, rischio che nella Scheda Violazione Dati (ALL. B) sarà stato classificato come **"NULLO"**.

Qualora la notifica all'Autorità di Controllo sia effettuata oltre le 72 ore, essa va corredata dei motivi del ritardo.

La notifica al Garante deve:

- a) descrivere, ove possibile:
  - i. la natura della Violazione dei Dati Personali;
  - ii. le categorie ed il numero approssimativo di Interessati in questione;
  - iii. le categorie ed il numero approssimativo di registrazioni dei Dati Personali in questione;
- b) comunicare il nome e i Dati di contatto del RPD o di altro punto di contatto presso cui ottenere più informazioni;
- c) descrivere le probabili conseguenze della Violazione dei Dati Personali;
- d) descrivere le misure adottate o di cui si propone l'adozione da parte dell'Ente per porre rimedio alla Violazione dei Dati Personali e per attenuarne i possibili effetti negativi.

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.

La notifica deve essere effettuata avvalendosi della modulistica predisposta dal Garante (nome del file *"Modello notifica Data Breach"*) reperibile al seguente link: <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9128501>. Il modello deve essere compilato seguendo le istruzioni presenti sul sito del Garante, riportato su carta intestata dell'Ente e spedito per posta elettronica certificata.

##### 2. COMUNICAZIONE DELLA VIOLAZIONE ALL'INTERESSATO

Il Titolare **Comune di Calcinaia**, con la collaborazione del gruppo individuato e con il supporto del RPD, laddove la Violazione presenti un rischio elevato per i diritti e le libertà delle persone fisiche, deve informare gli Interessati dell'evento anomalo, a norma degli artt. 33-34 del GDPR.

La comunicazione deve essere rivolta all'Interessato senza ingiustificato ritardo dall'avvenuta conoscenza e valutazione della Violazione, attraverso il canale di comunicazione ritenuto più idoneo. Deve essere intellegibile, concisa, trasparente, e facilmente accessibile; utilizzando un linguaggio semplice e chiaro, e adottando, ove possibile, la stessa lingua parlata dall'Interessato.

La comunicazione di *Data Breach* all'Interessato deve contenere le seguenti informazioni:

- a. data e ora della Violazione, anche solo presunta, e data e ora in cui si è avuto conoscenza della stessa;



## Comune di Calcinaia

### Servizio Segreteria e Affari Generali

- b. la natura della Violazione dei Dati Personali;
- c. il nome e i Dati di contatto del RPD, se esistente, o di altro punto di contatto presso cui ottenere più informazioni;
- d. le probabili conseguenze della Violazione dei Dati Personali;
- e. la descrizione delle misure adottate o di cui si propone l'adozione da parte dell'Ente/Società per porre rimedio alla Violazione dei Dati Personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Deve essere valutata l'opportunità o meno di comunicare all'Interessato anche se è soddisfatta una delle seguenti condizioni:

- a. se erano state messe in atto misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai Dati Personali oggetto della Violazione, con particolare riguardo a quelle destinate a rendere i Dati Personali incomprensibili a chiunque non sia autorizzato ad accedervi, **quali la cifratura**; e salvo che la Violazione della sicurezza abbia comportato la distruzione o la perdita dei Dati Personali dell' Interessato;
- b. se sono state successivamente adottate misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà delle persone fisiche – in tal caso è necessario documentare le misure nella scheda Violazione Dati (ALL.B);

Ove la suddetta comunicazione richieda sforzi sproporzionati, si può procedere ad una comunicazione pubblica o a una misura simile, tramite la quale gli Interessati siano informati con analoga efficacia.

Si riporta in calce il **Modello di comunicazione all'Interessato** della Violazione dei Dati Personali (**Allegato 1**).

#### **D. FASE 4: REGISTRAZIONE SEGNALAZIONE NEL REGISTRO DEI "DATA BREACH"**

Nel Registro dei *Data Breach* (ALL. C), allegato alla presente procedura, il Titolare Comune di Calcinaia, con il coinvolgimento e il supporto del RPD, documenta ogni singolo evento, sia esso, **FALSO POSITIVO, IRRILEVANTE, RILEVANTE** ovvero **GRAVE**; **in quest'ultimi tre casi**, devono essere indicate nel registro:

- le conseguenze del *Data Breach*;
- i provvedimenti adottati per porvi rimedio o attenuarne le conseguenze;
- l'eventuale notificazione all'Autorità di Controllo;
- l'eventuale comunicazione all'Interessato.

Tale documentazione consente all'Autorità di Controllo di verificare il rispetto delle norme in materia di notificazione delle Violazioni di Dati Personali.

Il Registro dei *Data Breach*, così come tutta la documentazione relativa alla Violazione verificatasi (Schede Evento e Scheda Violazione Dati) sono tenuti a cura del Titolare del Trattamento dei dati, presso l'USP, sotto il controllo del RPD/DPO.

#### **E. FASE 5: ANALISI POST VIOLAZIONE**

L'ultima fase del processo di gestione delle Violazioni di Dati Personali prevede la raccolta finale delle evidenze, l'analisi delle informazioni giunte a seguito dell'evento di Violazione registrato e la valutazione delle stesse al fine di effettuare un'analisi post-incidente, verificare l'efficacia e l'efficienza delle azioni intraprese durante la gestione dell'evento ed identificare possibili aree di miglioramento.

## **Comune di Calcinaia**

### **Servizio Segreteria e Affari Generali**

Anche tale attività prevede il coinvolgimento, laddove necessario, del servizio Informativo dell'Unione Valdera e l'eventuale supporto di tutti i servizi dell'Ente.

#### **IV. DESCRIZIONE PROCESSO: "DATA BREACH" PRESSO L'ENTE O UN TERZO IN QUALITÀ DI RESPONSABILE ESTERNO O IN CASO DI CONTITOLARITA'**

##### **A. OBBLIGHI DI COMUNICAZIONE DELL' ENTE QUANDO OPERA IN QUALITÀ DI RESPONSABILE ESTERNO**

Quando l'Ente Comune di Calcinaia agisce in qualità Responsabile esterno, in caso di Violazione dei Dati Personali, deve informare il Titolare (ovvero il soggetto per il quale tratta i dati e/o è tenuto a trattarli), senza ingiustificato ritardo secondo i tempi e i modi concordati nel contratto per il Trattamento dei Dati Personali trasmesso da quest'ultimo.

##### **B. OBBLIGHI DI COMUNICAZIONE DI UN RESPONSABILE ESTERNO NEI CONFRONTI DELL'ENTE**

Al verificarsi di una Violazione dei Dati Personali presso uno dei Responsabili esterni nominati dal Comune di Calcinaia, il Responsabile esterno deve informare il Titolare del trattamento Comune, senza ingiustificato ritardo e non oltre le 24/36 ore dal momento in cui ha conoscenza della Violazione, inviando una comunicazione ai seguenti indirizzi di posta elettronica: \_\_\_\_ pec: \_\_\_\_ e immediatamente collaborare con l'Ente per consentire allo stesso di adempiere agli obblighi previsti dalla normativa agli artt. 33 e 34 del GDPR.

La notifica del Responsabile al Titolare deve contenere almeno una descrizione della natura della violazione di dati personali comprensiva dei seguenti elementi:

- le categorie e il numero approssimativo di interessati coinvolti;
- le categorie e il numero approssimativo di dati personali coinvolti;
- il livello della gravità della violazione;
- le misure di sicurezza messe in atto;
- il nome e i dati di contatto del Responsabile della Protezione dei Dati – eventualmente designato dal Responsabile - o altro punto di contatto dal quale possono essere ottenute ulteriori informazioni;
- il nome e i dati di contatto del Responsabile della Protezione dei Dati – eventualmente designato dai Sub-responsabili coinvolti nel Trattamento - o altro punto di contatto dal quale possono essere ottenute ulteriori informazioni;
- la descrizione delle misure che il Responsabile intende adottare per porre rimedio alla violazione dei Dati, tra cui, se del caso, misure destinate ad attenuare le possibili conseguenze negative;
- la descrizione delle probabili conseguenze della violazione dei Dati;
- ogni ulteriore informazione necessaria affinché il Titolare possa notificare la violazione all'Autorità di controllo competente nei termini previsti dal GDPR.

Il Responsabile si impegna sin d'ora a collaborare con il Titolare per consentirgli la migliore e regolare gestione di ogni evento, anche solo potenziale, di violazione dei dati personali.

In ogni caso, il Responsabile assicura al Titolare del trattamento la massima collaborazione per

## Comune di Calcinaia

### Servizio Segreteria e Affari Generali

approfondire tutti gli aspetti necessari ed utili ad accertare le cause e le conseguenze della violazione. Una volta definite le ragioni della violazione, il Responsabile di concerto con il Titolare si attiverà per implementare nel minor tempo possibile tutte le misure di sicurezza fisiche e/o logiche e/o organizzative atte ad arginare il verificarsi di una nuova violazione della stessa specie di quella verificatasi. L'evento deve essere inserito dall'Ente Comune nell'apposito **Registro dei Data Breach** il cui modello è allegato alla presente procedura. L'Ente, una volta ricevuta la segnalazione deve procedere secondo le prescrizioni di cui ai alla presente procedura.

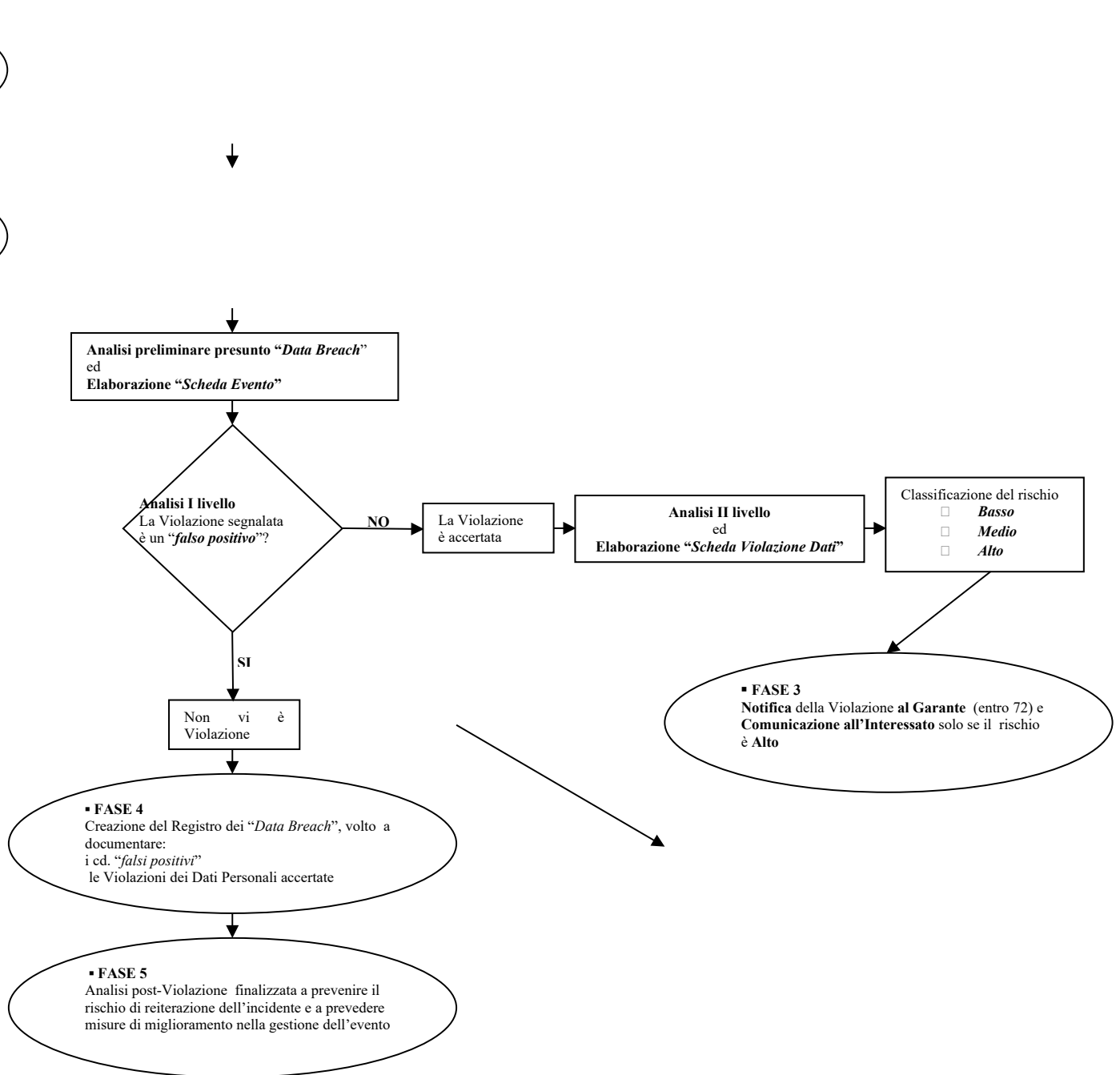
#### **C. OBBLIGHI DI COMUNICAZIONE IN CASO DI CONTITOLARITA' DEL TRATTAMENTO**

Ove il Comune di Calcinaia sia Contitolare con altri Enti di un trattamento di dati personali, la notifica al Garante per la protezione dei Dati Personali sarà a carico del Contitolare che per primo viene a conoscenza della violazione. Lo stesso informerà preventivamente l'altro Contitolare affinché entrambi, a seguito dell'analisi della segnalazione, possano concordare eventuali azioni congiunte tra cui appunto la necessità di notifica al Garante nonché la necessità di comunicazione all'interessato.

Comune di Calcinaia  
Servizio Segreteria e Affari Generali

DIAGRAMMA PROCESSO DI GESTIONE DATA BREACH

Il diagramma che segue riporta, in maniera sintetica, le fasi del Processo di gestione dei "Data Breach", sopra descritto:



**Comune di Calcinaia**  
**Servizio Segreteria e Affari Generali**

**V ALLEGATI**

**ALL. A:** SCHEDA EVENTO;

**ALL. B:** SCHEDA VIOLAZIONE DATI

**ALL. C:** REGISTRO DEI DATA BREACH

**ALL. D:** “MODELLO DI COMUNICAZIONE ALL’INTERESSATO DELLA VIOLAZIONE DEI DATI PERSONALI”

**Comune di Calcinaia**  
**Servizio Segreteria e Affari Generali**

**ALL. A -SCHEDA EVENTO**

SCHEDA EVENTO					
EVENTO				PROVVEDIMENTI	
DATA EVENTO		DATA E ORA DI CONOSCENZA		NOTIFICA AL GARANTE (X)	
ORA EVENTO		SEGNALANTE		SI	NO
LUOGO DELLA VIOLAZIONE		NATURA EVENTO		(inserire data di notifica)	(motivare mancata notifica)
ENTE/SOCIETA' COINVOLTO/A		N. INTERESSATI COINVOLTI			
CATEGORIE DI DATI INTERESSATI		CATEGORIE DI INTERESSATI COINVOLTI		(eventuale) COMUNICAZIONE ALL'INTERESSATO	
				SI	NO
				(inserire data di comunicazione)	(motivare mancata comunicazione)
				INTERVENTI DI RIPRISTINO (RECOVERY)	
CONSEGUENZE VIOLAZIONE		SISTEMI E DISPOSITIVI COINVOLTI			
				TEMPO DI RIPRISTINO (RECOVERY)	
DESCRIZIONE ANALITICA DELL'EVENTO				ULTERIORI AZIONI DA INTRAPRENDERE	
CODICE EVENTO					
DATA DI COMPILAZIONE				FIRMA	
LUOGO DI COMPILAZIONE					

**Comune di Calcinaia**  
**Servizio Segreteria e Affari Generali**

**ALL. B -SCHEDA VIOLAZIONE DATI**

CODICE EVENTO	CLASSIFICAZIONE RISCHIO	LIVELLO DI RISCHIO	CLASSIFICAZIONE EVENTO

Il rischio va riferito alla probabilità che si verifichi una delle seguenti condizioni a danno di persone fisiche anche diverse dall'interessato a cui si riferiscono i dati, a causa della violazione dei dati personali:

- 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
- danno economico o sociale significativo
- privazione o limitazione di diritti o libertà
- impedito controllo sui dati personali all'interessato
- danni fisici, materiali o immateriali alle persone fisiche.

N.B. Griglia di classificazione

Gravità della Violazione	Classificazione del rischio	Livello di Rischio	Classificazione evento
TRASCURABILE	NULLO	R1	Falso Positivo (FP)
BASSA	BASSO	R2	Irrilevante (I)
ALTA	ALTO	R3	Rilevante (R)
MOLTO ALTA	MOLTO ALTO	R4	Grave (G)

**Comune di Calcinaia**  
**Servizio Segreteria e Affari Generali**

**ALL. C - REGISTRO DEI DATA BREACH**

REGISTRO DELLE VIOLAZIONI DI DATI PERSONALI (DATA BREACH)											
n .	Data	Codice Evento	N. interessati Coinvolti	Notifica al Garante (X)		Comunicazione agli Interessati (X)		Livello Rischio	Classifica Evento FP/I/R/G	Conseguenze	Provvedimenti adottati
				SI	NO	SI	NO				
1				SI	NO	SI	NO				
				(data notifica)	(motivo mancata notificazione)	(data comunicazione)	(motivo mancata notificazione)				
2				SI	NO	SI	NO				
				(data notifica)	(motivo mancata notificazione)	(data comunicazione)	(motivo mancata notificazione)				
3				SI	NO	SI	NO				
				(data notifica)	(motivo mancata notificazione)	(data comunicazione)	(motivo mancata notificazione)				
4				SI	NO	SI	NO				
				(data notifica)	(motivo mancata notificazione)	(data comunicazione)	(motivo mancata notificazione)				
5				SI	NO	SI	NO				
				(data notifica)	(motivo mancata notificazione)	(data comunicazione)	(motivo mancata notificazione)				



**Comune di Calcinaia**  
**Servizio Segreteria e Affari Generali**

*Allegato 1*

**MODELLO DI COMUNICAZIONE ALL'INTERESSATO DELLA VIOLAZIONE DEI DATI PERSONALI**

*(Nota: Il seguente modello illustra le modalità di comunicazione di una Violazione. Rispetto ai diversi campi indicati dovrà essere scelta l'opzione che si può riferire allo specifico caso, in base agli esempi riportati)*

Prot. n.

Egr. Sig./ra.....

**Oggetto:** Comunicazione di violazione dei dati personali.

*Egr. Interessato,*

*secondo quanto prescritto dall'art. 34 del Regolamento Generale in materia di protezione dei dati personali RE (UE) n. 679/2016, l'Ente **Comune di Calcinaia**, in qualità di Titolare del Trattamento dei Suoi Dati, Le comunica l'intervenuta Violazione dei Suoi Dati Personali (Data breach)*

- *che si è verificata:*

- A. in data \_\_\_\_\_, alle ore \_\_\_\_\_;
- B. tra il \_\_\_\_\_ e il \_\_\_\_\_;
- C. in un tempo non ancora determinato;
- D. è possibile che sia ancora in corso.

- *di cui si è avuto conoscenza in data \_\_\_\_\_ alle ore \_\_\_\_\_.*

**A) Descrizione della natura della Violazione:**

---

---

---

---

---

---

a) Dove è avvenuta la Violazione dei Dati? (Specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili).

---

---

---

b) Tipo di Violazione, per esempio:

- 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)

**Comune di Calcinaia**  
**Servizio Segreteria e Affari Generali**

- furto (i Dati non sono più sui sistemi del Titolare e li ha l'autore della Violazione)
- altro \_\_\_\_\_

c) Dispositivo oggetto di Violazione, per esempio:

- computer
- rete
- dispositivo mobile
- strumento di backup
- documento cartaceo
- altro \_\_\_\_\_

d) Descrizione dei sistemi di elaborazione o di memorizzazione dei Dati coinvolti, con indicazione della loro ubicazione:

---

---

---

---

---

---

e) Che tipo di Dati sono oggetto di Violazione, per esempio:

- Dati anagrafici (nome, cognome, numero di telefono, e mail, CF, indirizzo ecc..)
- Dati di accesso e di identificazione (username, password, customer ID, altro)
- Dati personali idonei a rivelare l'origine razziale ed etnica
- Dati personali idonei a rivelare le convinzioni religiose
- Dati personali idonei a rivelare filosofiche o di altro genere
- Dati personali idonei a rivelare le opinioni politiche
- Dati personali idonei a rivelare l'adesione a partiti
- Dati personali idonei a rivelare sindacati,
- Dati personali idonei a rivelare associazioni od organizzazioni a carattere religioso
- Dati personali idonei a rivelare associazioni od organizzazioni a carattere filosofico
- Dati personali idonei a rivelare associazioni od organizzazioni a carattere politico
- Dati personali idonei a rivelare associazioni od organizzazioni a carattere sindacale
- Dati personali idonei a rivelare lo stato di salute
- Dati personali idonei a rivelare la vita sessuale
- Dati giudiziari
- Dati genetici
- Dati biometrici
- Copia per immagine su supporto informatico di documenti analogici
- Ancora sconosciuto
- Altro \_\_\_\_\_

**B) Descrivere le probabili conseguenze della Violazione dei Dati Personali;**

---

---

---

**Comune di Calcinaia**  
**Servizio Segreteria e Affari Generali**

C) Descrivere quali sono le misure tecnologiche ed organizzative assunte per porre rimedio alla Violazione e, se del caso, per contenere la Violazione dei Dati o per attenuarne i possibili effetti negativi;

---

---

---

Per poter ottenere maggiori informazioni relativamente alla Violazione in oggetto, può scrivere ai seguenti indirizzi di posta elettronica: \_\_\_\_\_ pec: \_\_\_\_\_;

Dati di contatto:

- a) nome e cognome del RPD: **avv.to Flavio Corsinovi**,
- b) indirizzo di posta elettronica: \_\_\_\_\_
- c) indirizzo di posta PEC: \_\_\_\_\_
- d) indirizzo posta cartacea: **Piazza Indipendenza 7 Calcinaia**
- e) numero telefonico dedicato: \_\_\_\_\_
- d) Unità di Supporto privacy del Comune di Calcinaia. Mail: \_\_\_\_\_ Tel: 0 \_\_\_\_\_

*Distinti saluti*

**Data, Luogo** \_\_\_\_\_

***Il Titolare del Trattamento***

\_\_\_\_\_

***Il Responsabile della Protezione dei Dati del Comune di Calcinaia***

\_\_\_\_\_

## **GLOSSARIO E ACRONIMI**

- **«Aree Sensibili»:** sono quei luoghi fisici o della Rete Aziendale in cui vengono Trattati Dati Particolari e/o Dati Giudiziari relativi a persone fisiche; e/o luoghi in cui vengono gestiti e consultati documenti riservati a cui è assolutamente vietato accedere se non per motivi di servizio.
- **«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.
- **«Autorità di Controllo»:** l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del GDPR.
- **«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.
- **«Dati Personali»:** 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 ad 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.
- **«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 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 Giudiziari»:** Dati Personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza.
- **«Dati Particolari»:** Dati Personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi ad identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
- **«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.
- **«Destinatario/i»:** 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

## Comune di Calcinaia

### Servizio Segreteria e Affari Generali

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.

- **«Device Fissi»:** si intendono gli strumenti informatici non facilmente removibili dal perimetro aziendale quali personal computer, server locali, stampanti affidati alle Persone Autorizzate per uso professionale.
- **«Device Mobili»:** in generale si intendono quegli strumenti informatici che per loro natura sono facilmente asportabili dal perimetro aziendale quali chiavette USB, SD cards, hard disk esterni, tablet e smartphone utilizzati dalla Persone Autorizzate per uso professionale.
- **«RPD o DPO - Data Protection Officer»:** è una persona fisica, nominata obbligatoriamente nei casi di cui all'art. 37.1 GDPR dal Titolare o dal Responsabile del Trattamento e deve possedere una conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati per assisterli nel rispetto a livello interno del GDPR.
- **«Gruppo Imprenditoriale»:** un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate.
- **«Persona/e Autorizzata/e al trattamento»:** si tratta dei Collaboratori autorizzati al Trattamento dei Dati Personali sotto la diretta autorità del Titolare e/o del Responsabile ex artt. 4(10) e 29 del GDPR. Stante la definizione fornita dal Gruppo di Lavoro Articolo 29 dell'Opinione 2/2017 questa definizione ricomprende: dipendenti ed ex dipendenti, dirigenti, sindaci, collaboratori e lavoratori a partita IVA, lavoratori a chiamata, part-time, *job-sharing*, contratti a termine, stage, senza distinzione di ruolo, funzione e/o livello, nonché consulenti e fornitori della Società e, più in generale, tutti coloro che utilizzino od abbiano utilizzato Strumenti Aziendali o Strumenti Personali operino sulla Rete ovvero siano a conoscenza di informazioni aziendali rilevanti quali, a titolo esemplificativo e non esaustivo: (a) i Dati Personali di clienti, dipendenti e fornitori, compresi gli indirizzi di posta elettronica; (b) tutte le informazioni aventi ad oggetto informazioni confidenziali di natura commerciale, finanziaria o di strategia di business; nonché (c) i dati e le informazioni relative ai processi aziendali, inclusa la realizzazione di marchi, brevetti e diritti di proprietà industriale, la cui tutela prescinde dagli effetti pregiudizievoli che potrebbe comportare la diffusione delle medesime.
- **«Limitazione Di Trattamento»:** il contrassegno dei Dati Personali conservati con l'obiettivo di limitarne il Trattamento in futuro.
- **«Processo Decisionale Automatizzato»:** decisione basata unicamente sul Trattamento automatizzato, compresa la Profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.
- **«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.

## Comune di Calcinaia

### Servizio Segreteria e Affari Generali

- **«Pseudonimizzazione»:** il Trattamento dei Dati Personali in modo tale che gli stessi non possano più essere attribuiti ad un Interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che queste ultime siano conservate separatamente e soggette a misure tecniche ed organizzative intese a garantire che tali Dati Personali non siano attribuiti ad una persona fisica identificata o identificabile.
- **«Rappresentante»:** la persona fisica o giuridica stabilita nell'Unione che, designata dal Titolare del Trattamento o dal Responsabile del Trattamento per iscritto ai sensi dell'articolo 27 GDPR, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del GDPR.
- **«Responsabile del Trattamento o Responsabile»:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta Dati Personali per conto del Titolare del Trattamento; deve presentare garanzie sufficienti di attuare misure tecniche e organizzative adeguate in modo tale che il Trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'Interessato.
- **«Rete»:** rappresenta il perimetro digitale della Società contenente Dati Personali e/o informazioni riservate comprensivo della rete interna (intranet) e della rete esterna (internet) a cui ci si può collegare via rete LAN, Wi-Fi o VPN.
- **«Sistema Informativo Aziendale»:** rappresenta il perimetro digitale della Società contenente Dati Personali e/o informazioni riservate fruibili dalla rete interna (intranet) e/o dalla rete esterna (internet).
- **«Soggetto designato al trattamento»:** la persona fisica, espressamente designata dal Titolare o dal Responsabile del trattamento sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, a specifici compiti e funzioni connessi al trattamento di dati personali e che opera sotto l'autorità diretta del Titolare o del Responsabile. Questi ultimi individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta.
- **«Strumenti Aziendali»:** l'insieme di Device Fissi e Device Mobili concessi in comodato d'uso dalla Società alle Persone Autorizzate al fine di svolgere le proprie mansioni.
- **«Strumenti Personali»:** i Device di proprietà delle Persone Autorizzate autorizzati ad essere impiegati per uso professionale.
- **«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.
- **«Titolare del Trattamento o Titolare»:** 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 o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.
- **«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.

**Comune di Calcinaia**  
**Servizio Segreteria e Affari Generali**

- **«Trattamento Transfrontaliero»:** a) 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 o il Responsabile siano stabiliti in più di uno Stato membro; oppure, b) Trattamento di Dati Personali che ha luogo nell'ambito delle attività di un unico stabilimento di un Titolare o Responsabile nell'Unione, ma che incide o probabilmente incide in modo sostanziale su Interessati in più di uno Stato membro.
- **«Violazione Dei Dati Personali ovvero Data Breach»:** è 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.