



Allegato n. 17 - Processo di analisi del data breach

In caso di accertamento di violazione che rientra nella definizione di Data Breach occorre seguire i seguenti passaggi relativi al processo di analisi:

1. Acquisizione della notizia da parte del soggetto preposto al ricevimento della violazione (Segretario Generale o altro soggetto preposto) che provvederà ad attivare i passi successivi;
2. Analisi tecnica dell'evento (ALLEGATO A);
3. Valutazione della gravità dell'evento (ALLEGATO B);
4. Notifica al Garante Privacy (se necessario);
5. Comunicazione agli Interessati (se necessario);
6. Altre segnalazioni dovute;
7. Inserimento dell'evento nel Registro delle Violazioni (ALLEGATO C);
8. Azioni correttive specifiche e per analogia (ALLEGATO D).

1. ACQUISIZIONE DELLA NOTIZIA

La segnalazione di un Data Breach può essere interna o esterna all'Ente.

- **INTERNA:** intesa come segnalazione proveniente da:
 - Personale dipendente
 - Personale convenzionato/stagisti/tirocinanti, ecc.
- **ESTERNA:** intesa come segnalazione proveniente da:
 - Responsabili del trattamento
 - Responsabile della protezione dei dati (RPD)
 - Interessati
 - Organi Pubblici (Agid, Polizia, altre Forze dell'Ordine, giornalisti, ecc.)
 - Altri soggetti

La segnalazione deve essere inoltrata al Segretario Generale o altro soggetto preposto, in forma libera, mediante:

- Posta elettronica;
- Avvertimento verbale/telefonico (in questo caso il Segretario Generale o il soggetto preposto redigerà un verbale sull'oggetto della segnalazione e del segnalante).

Dal momento in cui il soggetto preposto predetto viene a conoscenza dell'evento, decorre il termine



COMUNE di SENIGALLIA PROVINCIA di ANCONA

delle 72 ore previsto dalla normativa per l'invio dell'eventuale notifica all'Autorità di controllo.

2. ANALISI TECNICA DELL'EVENTO

Il Segretario Generale o il soggetto preposto in collaborazione con altri soggetti che il Segretario/soggetto preposto stesso ritiene opportuno coinvolgere (ad esempio Amministratore di sistema/responsabile del sistema informatico, responsabile del settore coinvolto, ecc.) e sentito il Responsabile della protezione dei dati (RPD), una volta verificato che l'evento segnalato si configuri effettivamente come un "Data Breach" darà seguito a tutte le attività, successivamente elencate, finalizzate a raccogliere gli elementi per una valutazione dell'evento (Analisi tecnica dell'evento – Allegato A) ai fini della notifica o meno al Garante della Privacy.

Nello specifico le attività da realizzare sono quelle previste nell'allegato A che deve essere compilato in ogni sua sezione, in un tempo consigliabile non superiore a 8 – 10 ore dall'avvenuta segnalazione, e riguardano ad esempio:

- Il riconoscimento della natura della violazione (distruzione, perdita, modifica, divulgazione non autorizzata o accesso ai dati personali trasmessi, conservati o comunque trattati);
- L'identificazione delle categorie di dati personali oggetto della violazione;
- L'identificazione delle categorie di Interessati oggetto della violazione;
- L'individuazione delle misure tecniche e organizzative adottate a seguito della violazione.

3. VALUTAZIONE DELLA GRAVITÀ DELL'EVENTO

Una volta realizzata l'analisi tecnica dell'evento oggetto di data breach il Segretario Generale/soggetto preposto, insieme ai soggetti coinvolti nella fase di analisi tecnica (fase 2) dovrà, attraverso la compilazione dell'allegato B, individuare se l'evento debba essere notificato al Garante della privacy (ed eventualmente anche agli interessati) oppure no.

In particolare, tramite l'allegato B, verrà valutata la gravità della violazione, cioè verrà valutato se la violazione possa comportare un rischio elevato o meno per i diritti e le libertà delle persone interessate.

La gravità della violazione è data dai seguenti fattori:

1. Categoria di dati personali;
2. Possibilità di identificare l'interessato;



COMUNE di SENIGALLIA PROVINCIA di ANCONA

3. Circostanze della violazione.

Qualora non si abbia un quadro completo della violazione si può attendere fino ad un massimo di 72 ore prima di effettuare la notifica al Garante. Alla scadenza delle 72 ore occorre comunque procedere ad avviare il processo di notifica effettuando una comunicazione preliminare riservandosi di effettuare una successiva notifica integrativa.

4. NOTIFICA AL GARANTE DELLA PRIVACY

Nel caso in cui, a seguito della valutazione della gravità della violazione (ALLEGATO B), venga evidenziato un probabile rischio per i diritti e le libertà delle persone fisiche occorre procedere alla comunicazione al Garante per la protezione dei dati personali in quanto in base 33 del GDPR, la notifica al Garante è resa obbligatoria nei casi in cui si verifichi una violazione dei dati personali, a meno che sia improbabile che tale violazione presenti un rischio per i diritti e le libertà delle persone fisiche.

La notifica è effettuata dal Segretario Generale/soggetto preposto, sentito il Responsabile della protezione dati (RPD), tramite un'apposita procedura telematica disponibile sul sito web del Garante Privacy. Le informazioni necessarie per la compilazione della procedura sono rinvenibili dagli allegati A e B.

A partire dal 1° luglio 2021, la notifica di una violazione di dati personali deve essere inviata al Garante tramite l'apposita procedura telematica, resa disponibile nel portale dei servizi online dell'Autorità, e raggiungibile all'indirizzo <https://servizi.gpdp.it/databreach/s/> (VEDI: Provvedimento del 27 maggio 2021).

Nella stessa pagina è disponibile un modello facsimile, da NON utilizzare per la notifica al Garante ma utile per vedere in anteprima i contenuti che andranno comunicati al Garante.

Nella notifica dovranno essere indicate le informazioni relative all'eventuale comunicazione agli interessati provenienti dalla realizzazione della fase 5.

5. COMUNICAZIONE AGLI INTERESSATI

Nel caso in cui, a seguito della valutazione della gravità della violazione (ALLEGATO B), venga evidenziato un rischio elevato (alto) per i diritti e le libertà delle persone fisiche, si provvederà ad informare gli interessati sul fatto avvenuto, sui dati violati e sulle procedure necessarie a ridurre il rischio.



COMUNE di SENIGALLIA PROVINCIA di ANCONA

La comunicazione, in formato libero, deve contenere, ai sensi dell'art. 34 del GDPR, le seguenti informazioni:

- a) il nome e i dati di contatto del Responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- b) la descrizione delle probabili conseguenze della violazione dei dati personali;
- c) la descrizione delle 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 attenuare i possibili effetti negativi.

Qualora la comunicazione a ciascun singolo interessato comporti sforzi sproporzionati, in base all'art. 34, par. 3, lett. c del GDPR, si può procedere invece ad una comunicazione pubblica o a una misurazione simile, tramite la quale gli interessati sono informati con analoga efficacia (come ad esempio sito web, quotidiani, radio e tv).

Della comunicazione agli interessati deve essere prodotta e conservata appropriata documentazione. Tale comunicazione, in base all'art. 34, par. 3 del GDPR, non è richiesta qualora il titolare del trattamento abbia successivamente adottato misure atte scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati. Di tali misure occorre darne evidenza nella notifica al Garante.

6. ALTRE SEGNALAZIONI DOVUTE

Il Segretario Generale/soggetto preposto, sentito il Responsabile della protezione dati (RPD), dovrà verificare la necessità di informare altri organi quali ad esempio:

- CERT-PA (in caso di incidenti informatici ai sensi della Circolare Agid n. 2/2017 del 18.04.2017);
- Organi di Polizia (in caso di violazioni di dati conseguenza di comportamenti illeciti o fraudolenti); Di tali comunicazioni occorre darne evidenza nella notifica al Garante.

7. INSERIMENTO DELL'EVENTO NEL REGISTRO DELLE VIOLAZIONI

In base all'art. 33 paragrafo n. 5 del GDPR, il titolare del trattamento deve documentare qualsiasi violazione dei dati personali, al fine di consentire all'Autorità di controllo di verificare il rispetto dell'art. stesso. Pertanto, il Segretario Generale/soggetto preposto dovrà annotare tutto quanto effettuato nelle fasi precedenti nel registro delle violazioni (ALLEGATO C). Tutti gli allegati dovranno essere numerati seguendo l'ordine progressivo delle violazioni annotate nel registro delle violazioni e archiviate negli appositi archivi cartacei o informatici.



**COMUNE di SENIGALLIA
PROVINCIA di ANCONA**

8. AZIONI CORRETTIVE SPECIFICHE O PER ANALOGIA

Le azioni previste in questa fase sono:

- Analisi della relazione dettagliata sull'incidente;
- Reiterazione del processo di Gestione del rischio informativo;
- Eventuale revisione di questo documento (se necessario) e di eventuali altri documenti collegati (es. Analisi del rischio, Misure di sicurezza);
- Individuazione di controlli che diminuiscano la probabilità dell'incidente o i relativi impatti sul sistema colpito e su sistemi analoghi;
- Revisione del Sistema di Gestione della Privacy;
- Revisione delle relazioni con gli Interessati;
- Revisione annuale della procedura.

ALLEGATI:

- MODELLO PER LA RACCOLTA DELLE INFORMAZIONI (ANALISI TECNICA) - **ALLEGATO A**
- MODELLO VALUTAZIONE GRAVITÀ DATABREACH – **ALLEGATO B**
- REGISTRO DELLE VIOLAZIONI – **ALLEGATO C**
- AZIONI CORRETTIVE – **ALLEGATO D**



**COMUNE di SENIGALLIA
PROVINCIA di ANCONA**

MODELLO PER LA RACCOLTA DELLE INFORMAZIONI (ANALISI TECNICA)- ALLEGATO A

Dati del soggetto segnalante

Cognome: _____

Nome: _____

E-mail: _____

Recapito telefonico per eventuali comunicazioni: _____

Funzione rivestita: _____

Ulteriori soggetti coinvolti nel trattamento

Indicare i riferimenti di ulteriori soggetti coinvolti ed il ruolo svolto (contitolare o responsabile del trattamento), rappresentante del titolare non stabilito nell'Ue).

Denominazione: _____

Codice Fiscale/P.IVA: _____ ☐ Soggetto privo di C.F./P.IVA

Ruolo: ☐ Contitolare ☐ Responsabile ☐ Rappresentante

Denominazione: _____

Codice Fiscale/P.IVA: _____ ☐ Soggetto privo di C.F./P.IVA

Ruolo: ☐ Contitolare ☐ Responsabile ☐ Rappresentante

Denominazione: _____

Codice Fiscale/P.IVA: _____ ☐ Soggetto privo di C.F./P.IVA

Ruolo: ☐ Contitolare ☐ Responsabile ☐ Rappresentante

Denominazione: _____

Codice Fiscale/P.IVA: _____ ☐ Soggetto privo di C.F./P.IVA

Ruolo: ☐ Contitolare ☐ Responsabile ☐ Rappresentante

Informazioni di sintesi sulla violazione



COMUNE di SENIGALLIA
PROVINCIA di ANCONA

1. Indicare quando è avvenuta la violazione:

- ☐ Il _____
- ☐ Dal _____ (la violazione è ancora in corso)
- ☐ Il _____
- ☐ Dal _____ al _____
- ☐ In un tempo non ancora determinato
- ☐ Ulteriori informazioni circa le date in cui è avvenuta la violazione: _

2. Breve descrizione della violazione: _____

3. Natura della violazione:

- ☐ **Perdita di confidenzialità** (diffusione/accesso non autorizzato o accidentale – “divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati”)
- ☐ **Perdita di integrità** (modifica non autorizzata o accidentale – “modifica”)
- ☐ **Perdita di disponibilità** (impossibilità di accesso, perdita, distruzione non autorizzata o accidentale - “distruzione/perdita”)

4. Causa della violazione:

- ☐ Azione intenzionale interna



COMUNE di SENIGALLIA
PROVINCIA di ANCONA

- ☐ Azione accidentale interna
- ☐ Azione intenzionale esterna
- ☐ Azione accidentale esterna
- ☐ Sconosciuta

☐ Altro (specificare): _____

5. Categorie di dati personali oggetto della violazione:

- ☐ Dati anagrafici (nome, cognome, sesso, data di nascita, luogo di nascita, codice fiscale, ecc.)
- ☐ 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, ecc.)
- ☐ Dati di pagamento (numero di conto corrente, dettagli della carta di credito, ecc.)
- ☐ Dati relativi alla fornitura di un servizio di comunicazione elettronica (dati di traffico, dati relativi alla navigazione Internet, ecc.)
- ☐ 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, ecc.)
- ☐ 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
- ☐ Dati biometrici



COMUNE di SENIGALLIA
PROVINCIA di ANCONA

☐ Categorie ancora non determinate

☐ Altro: _____

6. Indicare il volume (anche approssimativo) dei dati personali oggetto della violazione:

☐ N. _____

☐ Circa N. _____

☐ Un numero (ancora) non definito di dati personali

7. Indicare la categoria di interessati oggetto della violazione:

☐ 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 (ad esempio vittime di violenze o abusi, rifugiati, richiedenti asilo)

☐ Categorie ancora non determinate

☐ Altro: _____

8. Numero (anche approssimativo) di interessati coinvolti nella violazione:

☐ N. _____ interessati

☐ Circa N. _____ interessati

☐ Un numero (ancora) sconosciuto di interessati



**COMUNE di SENIGALLIA
PROVINCIA di ANCONA**

Ulteriori informazioni sulla violazione

1. Descrizione dei sistemi e delle infrastrutture IT (Information Technology) coinvolti nell'incidente, con

indicazione della loro ubicazione:

- Documento cartaceo: _____

- File o parte di file: _____

- Rete (ad esempio mail): _____

- Computer: _____

- Dispositivo mobile (ad esempio pen drive, hard disk esterno, cellulare, ecc.): _____



COMUNE di SENIGALLIA
PROVINCIA di ANCONA

- Strumento di back-up: _____

- Altro: _____

2. Misure di sicurezza tecniche e organizzative adottate per garantire la sicurezza dei dati, dei sistemi e delle infrastrutture IT coinvolti:

- Misure organizzative in essere al momento della violazione:

- ☐ Nomina Persona Autorizzata al Trattamento
- ☐ Istruzioni per il trattamento impartite al Personale Autorizzato al Trattamento
- ☐ Formazione del Personale Autorizzato al Trattamento



COMUNE di SENIGALLIA
PROVINCIA di ANCONA

☐ Locali chiusi a chiave in assenza, anche momentanea, del personale in servizio

☐ Armadi chiusi a chiave

☐ Procedura creazione/modifica credenziali di accesso (password)

☐ Armadi chiusi a chiave

☐ Policy varie (indicare e descrivere la sezione collegata alla violazione): _____

☐ Altro: _____

• Misure tecniche in essere al momento della violazione:

☐ Credenziali di accesso/password

☐ Firewall

☐ Antivirus

☐ Pseudonimizzazione dei dati personali

☐ Cifratura dei dati personali

☐ Ripristino dei dati personali (disaster recovery)

☐ Gruppo di continuità

☐ Altro: _____



**COMUNE di SENIGALLIA
PROVINCIA di ANCONA**

Possibili conseguenze della violazione

1. Possibili conseguenze della violazione sugli interessati:

A. 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): _____

B. In caso di perdita di integrità:

- ☐ I dati sono stati modificati e resi inconsistenti
- ☐ I dati sono stati modificati mantenendo la consistenza
- ☐ Altro (specificare): _____

C. In caso di perdita di disponibilità:

- ☐ Mancato accesso a servizi
- ☐ Malfunzionamento e difficoltà nell'utilizzo di servizi
- ☐ Altro (specificare): _____



COMUNE di SENIGALLIA
PROVINCIA di ANCONA

Ulteriori considerazioni sulle possibili conseguenze: _____

2. Potenziali effetti negativi sugli 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): _____



COMUNE di SENIGALLIA
PROVINCIA di ANCONA

Misure adottate in seguito alla violazione

1. Misure tecniche e organizzative adottate (o, distinguendole, di cui si propone l'adozione) per porre rimedio alla violazione e ridurre gli effetti negativi per gli interessati:

2. Misure tecniche e organizzative adottate (o, distinguendole, di cui si propone l'adozione) per prevenire simili violazioni future:

PARTECIPANTI:

NOME E COGNOME	FIRMA



COMUNE di SENIGALLIA
PROVINCIA di ANCONA

--	--

Data _____



COMUNE di SENIGALLIA
PROVINCIA di ANCONA

MODELLO VALUTAZIONE GRAVITÀ DATABREACH – ALLEGATO B

CATEGORIA DATI PERSONALI (A)

CATEGORIA DATI		DESCRIZIONE	PUNTEGGIO attribuibile	Punteggio attribuito*
<u>DATI PERSONALI COMUNI</u> Dati anagrafici, dati sull'istruzione, vita familiare, esperienza professionale, ecc.	A	Il contenuto della violazione riguarda soli dati "comuni" ed il titolare non è a conoscenza di alcun fattore aggravante.	1	
	B	Quando il volume di "dati comuni" e / o le caratteristiche del titolare sono tali da consentire l'individuazione di determinati profili dell'interessato o può essere formulato un profilo sullo stato sociale/finanziario dell'interessato.	2	
	C	Quando i "dati comuni" e / o le caratteristiche del titolare possono portare a supposizioni sullo stato di salute dell'individuo, sulle preferenze sessuali, sulle convinzioni politiche o religiose.	3	
	D	Quando a causa di determinate caratteristiche dell'individuo (ad es. gruppi vulnerabili, minori), l'informazione può essere critica per la sicurezza personale o per le condizioni fisiche / psicologiche.	4	
<u>DATI PERSONALI COMPORTAMENTALI</u> Dati sul traffico telefonico, dati sulle preferenze personali e abitudini, ecc.	A	Quando la natura dei dati violati non fornisce alcuna comprensione sostanziale delle informazioni comportamentali dell'individuo o i dati possono essere raccolti facilmente (indipendentemente dalla violazione) attraverso fonti disponibili pubblicamente (ad esempio combinazione di informazioni da ricerche web).	1	
	B	Violazione di dati comportamentali ed il titolare non è a conoscenza di fattori aggravanti.	2	
	C	Quando il volume di "dati comportamentali" e / o le caratteristiche del titolare sono tali da consentire la creazione di un profilo dell'individuo, esponendo informazioni dettagliate sulla sua vita quotidiana e sulle sue abitudini.	3	
	D	Quando i dati violati consentono di creare un profilo della persona basato su dati sensibili.	4	
<u>DATI PERSONALI FINANZIARI</u> Qualsiasi tipo di dati	A	I dati violati non forniscono alcuna comprensione sostanziale delle informazioni finanziarie dell'individuo (ad esempio il fatto che una persona sia il cliente di una determinata banca senza ulteriori dettagli).	1	
	B	I dati violati includono alcune informazioni finanziarie ma non forniscono informazioni significative sullo stato / sulla situazione finanziaria dell'individuo (ad esempio numeri di conti bancari semplici senza ulteriori dettagli).	2	
	C	Quando i dati violati consentono di creare un profilo della persona basato su dati sensibili.	3	



COMUNE di SENIGALLIA
PROVINCIA di ANCONA

finanziari (reddito, transazioni finanziarie, estratti conto bancari, ecc.)	D	I dati violati possono comportare la divulgazione di informazioni finanziarie complete (ad esempio carta di credito) che potrebbero consentire di frodare o creare un profilo sociale / finanziario dettagliato della persona.	4	
<u>DATI PERSONALI</u> <u>PARTICOLARI</u> (ex dati "sensibili")	A	I dati violati non forniscono alcuna comprensione sostanziale delle informazioni comportamentali dell'individuo o i dati possono essere raccolti facilmente (indipendentemente dalla violazione) attraverso fonti disponibili pubblicamente (ad esempio combinazione di informazioni da ricerche web).	1	
	B	I dati violati possono portare a ipotesi generali.	2	
	C	I dati violati possono portare a supporre informazioni sensibili.	3	
	D	Quando la violazione riguarda "dati sensibili".	4	
TOTALE PUNTEGGIO ATTRIBUITO AL FATTORE A:				

*attribuire un punteggio per ogni categoria di dati personali



COMUNE di SENIGALLIA
PROVINCIA di ANCONA

POSSIBILITÀ DI IDENTIFICAZIONE DELL'INTERESSATO (B)

LIVELLO	DESCRIZIONE		PUNTEGGIO ATTRIBUIBILE	Punteggio attribuito
TRASCURABILE	A	Con difficoltà si riesce ad abbinare i dati violati alla persona a meno che non sia abbia accesso ad altro database (ad esempio cifratura dei dati).	0,25	
LIMITATO	B	I dati violati potrebbero portare all'individuazione della persona.	0,50	
SIGNIFICATIVO	C	I dati violati consentono di rilevare più dati relativi alla persona ma non consentono di definire un profilo completo della persona.	0,75	
MASSIMO	D	I dati violati consentono di definire il profilo della persona.	1	
PUNTEGGIO ATTRIBUITO AL FATTORE B:				



COMUNE di SENIGALLIA
PROVINCIA di ANCONA

CIRCOSTANZE DELLA VIOLAZIONE **(C)**

CATEGORIA DATI	DESCRIZIONE		PUNTEGGIO ATTRIBUIBILE	Punteggio attribuito*
<u>PERDITA DI CONFIDENZIALITÀ</u> (diffusione/accesso non autorizzato o accidentale)	A	Dati esposti a rischi di riservatezza senza la prova che si sia verificata un'elaborazione illegale.	0	
	B	Dati portati a conoscenza di un numero limitato di soggetti.	0,25	
	C	Dati portati a conoscenza di un numero indefinito di soggetti.	0,50	
<u>PERDITA DI INTEGRITÀ</u> (modifica non autorizzata o accidentale)	A	Dati modificati ma senza aver rilevato alcun uso errato o illegale	0	
	B	Dati modificati ed eventualmente usati in modo errato o illegale ma con possibilità di recupero	0,25	
	C	Dati modificati ed eventualmente usati in modo errato o illegale senza possibilità di recupero	0,50	
<u>PERDITA DI DISPONIBILITÀ</u> (impossibilità di accesso, perdita, distruzione non autorizzata o accidentale)	A	Dati che possono essere recuperati senza difficoltà.	0	
	B	Dati che possono essere recuperati anche se con difficoltà.	0,25	
	C	Dati che non possono più essere recuperati.	0,50	



COMUNE di SENIGALLIA
PROVINCIA di ANCONA

<u>INTENTO MALEVOLO</u>	A	La violazione è dovuta a un'azione intenzionale al fine di causare problemi al titolare del trattamento dei dati.	0,50	
TOTALE PUNTEGGIO ATTRIBUITO AL FATTORE C:				

* in base alla natura della perdita individuata attribuire uno dei tre punteggi indicati per la perdita stessa ed eventualmente aggiungere il punteggio per l'intento malevolo (punteggio massimo attribuibile 1)



COMUNE di SENIGALLIA
PROVINCIA di ANCONA

STIMA DELLA GRAVITÀ DELLA VIOLAZIONE

A CATEGORIA DI DATI PERSONALI			Punteggio A: _____ X
B POSSIBILITÀ DI IDENTIFICAZIONE DELL'INTERESSATO			Punteggio B: _____
C CIRCOSTANZE DELLA VIOLAZIONE			TOT.: _____ + Punteggio C: _____
PUNTEGGIO TOTALE	NULLO TRASCURABILE BASSO MEDIO ALTO	< 1 $\geq 1 < 2$ $\geq 2 < 3$ $\geq 3 < 4$ ≥ 4	Punteggio TOTALE Gravità*: _____

PARTECIPANTI:



**COMUNE di SENIGALLIA
PROVINCIA di ANCONA**

NOME E COGNOME	FIRMA

Luogo e data _____

*Vedi legenda della gravità della violazione

LEGENDA DELLA GRAVITÀ DELLA VIOLAZIONE

Livello di gravità	Descrizione	Nessuna comunicazione	Comunicazione Garante	Comunicazione Interessati
NULLO	Rischio improbabile per gli interessati.	X		
TRASCURABILE	Gli individui non saranno interessati o potrebbero incontrare alcuni inconvenienti, che supereranno senza alcun problema.		X	



COMUNE di SENIGALLIA
PROVINCIA di ANCONA

BASSO	Gli individui possono incontrare notevoli disagi, che saranno in grado di superare nonostante alcune difficoltà.		X	
MEDIO	Gli individui possono incontrare conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà.		X	
ALTO	Gli individui possono incontrare conseguenze significative, o addirittura irreversibili, che non possono superare.		X	X



COMUNE di SENIGALLIA
PROVINCIA di ANCONA

REGISTRO DELLE VIOLAZIONI – ALLEGATO C

Titolare del trattamento:	COMUNE DI SENIGALLIA
Responsabile dalla protezione dei dati (RPD-DPO):	dpo@comune.senigallia.an.it

SEGNALEZIONE										INTERESSATI e DATI			
N.	Data e ora	Segnalante	Settore/Area coinvolto	Organi informati	Luogo violazione	Modalità violazione	Sistemi/apparati/reti/ banche dati oggetto di data breach	Natura della violazione dei dati personali	Altri elementi utili alla descrizione violazione	Categorie di interessati	Numero approssimativo di interessati	Categorie dei dati personali	Numero approssimativo di registrazioni dei dati personali
1													
2													



COMUNE di SENIGALLIA
PROVINCIA di ANCONA

CONSEGUENZE	RIMEDI		ATTENUAZIONE	TEMPI	ALLEGATO A	ALLEGATO B	NOTIFICA AL GARANTE							COMUNICAZIONE AGLI INTERESSATI			NOTE
Conseguenze della violazione dei dati personali	Misure adottate per porre rimedio alla violazione	Misure di cui si propone l'adozione per porre rimedio alla violazione	Misure adottate per attenuare i possibili effetti negativi	Misure di cui si propone l'adozione per attenuare i possibili effetti negativi	Tempo ripristino	Data e numero allegato A (Raccolta informazioni)	Data e numero allegato B (Modello valutazione gravità)	Completa	Preliminare	Integrativa	Ragioni dell'eventuale ritardo della notificazione	Ragioni di omessa notifica	N. Fascicolo	comunicazione agli interessati:	modalità della comunicazione e agli interessati	ragioni della omessa comunicazione agli interessati	



COMUNE di SENIGALLIA
PROVINCIA di ANCONA

AZIONI CORRETTIVE – ALLEGATO D

N. VIOLAZIONE	DATA DELLA VIOLAZIONE	AZIONE CORRETTIVA	DATA DI SCADENZA REALIZZAZIONE	RESPONSABILE DELL'AZIONE CORRETTIVA	
				NOME	RUOLO/MANSIONE