Procedura operativa relativa alla gestione delle violazioni di dati personali

Data	redazione	approvazione	autorizzazione	N° archiviazione
05/04/2019	Dott. sse Anna Laura Lacerra e Maria Cristina Vennera	Avv. Fabrizio Basso	Dott. Fabrizio Basso	n. Decreto n.

Sommario

DESTINATARI :

Dirigente	Segretario Generale
Responsabili d'Area	Responsabili esterni
Dipendenti	Collaboratori

1. Premessa

La violazione dei dati personali consiste nella violazione della sicurezza che comporta, in modo accidentale o illecito, la distruzione, la perdita, la modifica, la divulgazione o l'accesso non autorizzati ai dati personali trasmessi, conservati o comunque trattati.

L'art. 33 del Regolamento UE dispone che la notifica di violazione dei dati personali all'autorità di controllo debba essere effettuata dal Titolare del trattamento entro 72 ore dal momento in cui ne ha avuto conoscenza (sia in caso di conoscenza diretta, sia in caso di comunicazione da parte del responsabile esterno o dell'interessato o da qualunque altro soggetto), a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

Il termine di 72 ore non è puramente indicativo ma categorico, il suo mancato rispetto se non adeguatamente motivato, integra una situazione sanzionabile.

Il Titolare, ricevuta tale segnalazione, nel rispetto della procedura sotto riportata, notifica al Garante la violazione fornendogli tutte le informazioni previste nell'art. 33 del GDPR e indicando, inoltre, tutte le conseguenze che potrebbero derivare dalla violazione dei dati.

Il titolare del trattamento deve, inoltre, comunicare (senza ingiustificato ritardo) a ciascun interessato l'avvenuta violazione a meno che (art. 33 comma 4):

-non siano state adottate adeguate ed efficaci misure per mettere in sicurezza i dati (ad esempio cifratura);

-non si siano adottate misure per scongiurare il pericolo di limitazione per le libertà e i diritti delle persone fisiche;

-la comunicazione individuale sia troppo onerosa.

Chi viene a conoscenza di una violazione deve immediatamente segnalarla al responsabile di area attraverso la modulistica predisposta (cfr. Modello DB); questi ultimi a loro volta entro le 24 ore successive, dovranno raccogliere quante più informazioni possibili in modo da compilare in tutte le sue parti il Modello DB e trasmettere la notizia via e-mail al DPO, all'indirizzo **privacy@provincia.ancona.it**.

2. SCOPO

La procedura operativa descritta nel presente documento è finalizzata a definire in maniera chiara e comprensibile da tutto il personale interessato e dai responsabili esterni, il processo, le modalità operative, i ruoli e le responsabilità organizzative, che consentano un approccio esaustivo ed omogeneo nella gestione delle violazioni di sicurezza afferenti alla privacy, secondo i criteri ed i principi stabiliti dalle vigenti normative.

Con questo documento il Titolare del trattamento dei dati personali recepisce e pone in atto gli indirizzi cogenti formulati negli art. 32 e 33 del Regolamento UE 679/2016 e nei vari Regolamenti emessi dal Garante per la tutela dei dati personali.

3. CAMPO DI APPLICAZIONE

La procedura operativa si applica nello specifico alle Unità organizzative della Provincia di Ancona (Settori, Aree, Unità operative) che trattano a qualsiasi titolo e in qualsiasi modalità (automatizzata, manuale, digitale, cartacea) dati personali riconducibili alle seguenti categorie di Interessati:

- Personale a tempo indeterminato e determinato, collaboratori, consulenti;
- Utenti o fornitori.

4. TERMINOLOGIA, ABBREVIAZIONI, DEFINIZIONI

GDPR: General Data Protection Regulation - Regolamento (UE) 679/2016
DPO: Data Protection Officer – Responsabile della protezione dei dati
Titolare: Titolare del trattamento; il titolare è la Provincia di Ancona nel suo complesso, ma ai fini del presente documento è identificato nel Presidente pro - tempore;
Dati personali: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»);
Responsabili esterni: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

5. RUOLI E RESPONSABILITA'

Di seguito vengono descritti i soggetti protagonisti della procedura.

Chiunque: Tutto il personale della Provincia di Ancona a tempo determinato ed indeterminato, il Segretario Generale, il Dirigente, i collaboratori, i consulenti, i fornitori e i responsabili esterni che a vario titolo svolgono attività e servizi per conto dell'ente
Titolare: il Presidente pro-tempore, attualmente identificato nel Sig. Luigi Cerioni
DPO: Il Responsabile della protezione dei dati personali pro tempore, attualmente identificato nella Dott.ssa Anna Laura Lacerra
Garante Privacy: l'autorità garante per la protezione dei dati personali
Interessato: la persona fisica dei cui dati si tratta.

6. RIFERIMENTI

Regolamento (UE) 679/2016 (GDPR), linee guida sulla notifica delle violazioni dei dati personali del 3 ottobre 2017 ed emendate il 6 febbraio 2018 e Provvedimento del Garante del 2 luglio 2015

7. MOTIVAZIONI

La procedura intende porre rimedio nel più breve tempo possibile alle violazioni di dati personali che si dovessero verificare; laddove la violazione comporti un rischio per i diritti e le libertà fondamentali dell'individuo, la procedura permette di notificare la violazione al garante e di comunicare la violazione agli interessati nei termini di legge in un'ottica collaborativa e per permettere la immediata risoluzione della criticità.

8. DESCRIZIONE DELLE ATTIVITA'

Attività di segnalazione, raccolta informazioni, valutazione e notifica della violazione

Step	Attività	Chi	A chi	Quando	Come
1	Rilevazione della violazione	Chiunque rilevi la violazione		Appena ne viene a conoscenza	Forma libera
2	Segnalazione della violazione	Chiunque abbia rilevato la violazione	Al Responsabile di Area	Immediatamente	Utilizzando le vie più brevi (consegna a mano, email, ecc.) e possibilmente compilando, anche solo in parte, il modulo DB
3	Raccolta informazioni	Responsabile di Area		Appena ricevuta la segnalazione	Compilando il modulo DB
4	Comunicazione della violazione	Responsabile di Area	Al DPO	Appena compila il modulo DB	Tramite protocollo
5	Valutazione di impatto	Il DPO		Appena riceve il modulo DB	Forma libera
6	Individuazione azioni correttive	Il DPO		Terminata la valutazione di impatto	Forma libera
7	Comunicazione della valutazione	Il DPO	Al Titolare	Terminata la individuazione delle azioni correttive	Tramite protocollo
8	Documentazione della avvenuta violazione	Il Titolare		Appena ricevuta la valutazione di impatto	Utilizzando il registro delle violazioni
Condizioni: • il trattamento presenta probabili rischi per i diritti e le libertà delle persone fisiche					
9	Notificazione della violazione	Il Titolare	Al Garante Privacy	Entro 48 ore dalla conoscenza (non oltre 72 ore in casi eccezionali)	Tramite PEC all'indirizzo databreach.pa@pec.gpdp.it utilizzando il modulo DB

Step	Attività	Chi	A chi	Quando	Come
Condizioni: • il trattamento presenta probabili rischi per i diritti e le libertà delle persone fisiche • il probabile rischio è elevato • non si soddisfano le condizioni di cui all'art. 34 comma 3 del GDPR.					
10	Comunicazione della violazione	Il Titolare	Agli interessati	Senza ingiustificato ritardo	Forma libera ma con linguaggio semplice e chiaro

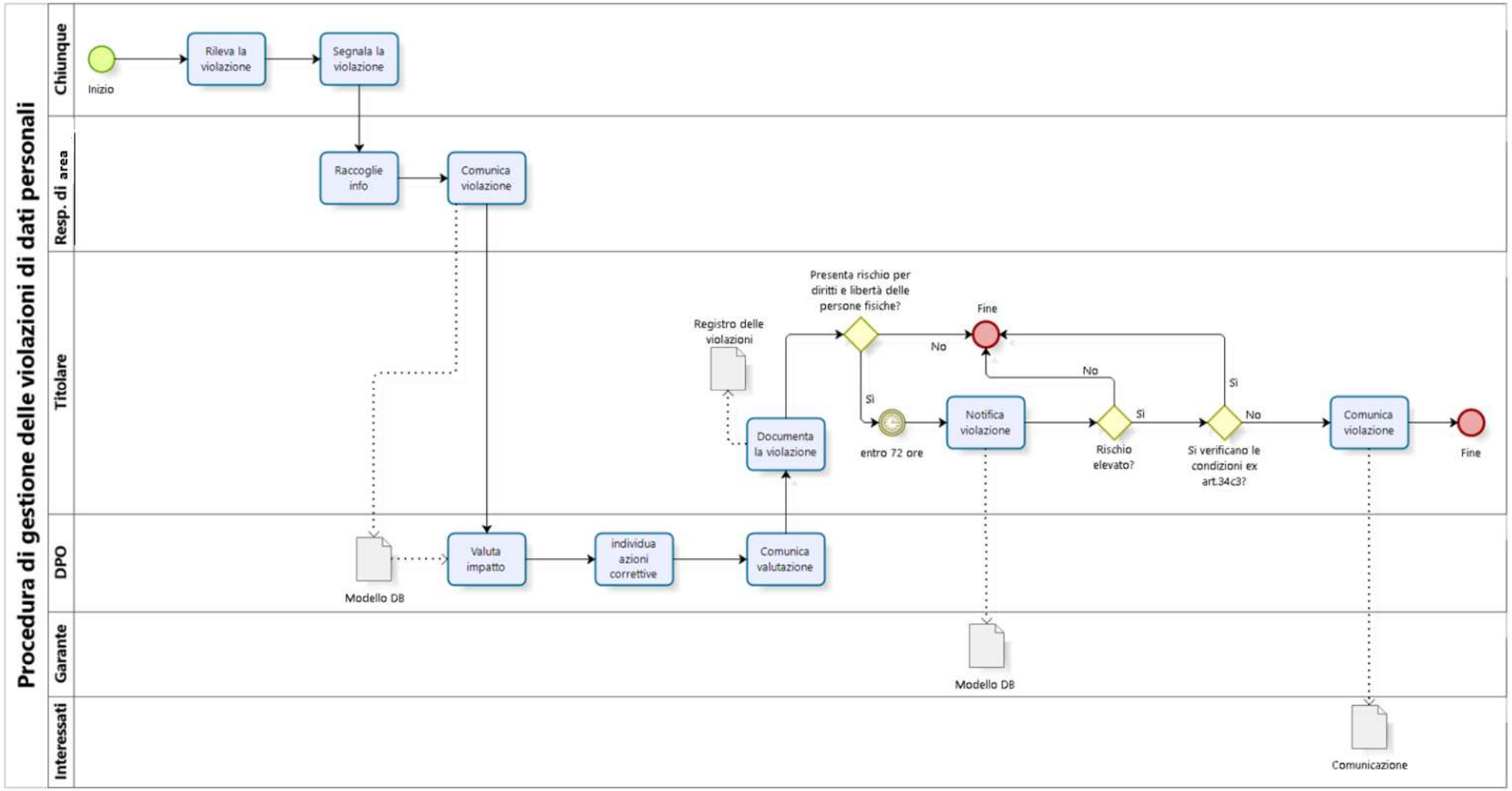
9. ARCHIVIAZIONE

Il presente documento è pubblicato sulla rete intranet della Provincia di Ancona Stamira nelle news per 30 giorni e in modalità permanente nella sezione dedicata alla Privacy

ALLEGATI E APPENDICI

1	**Modello DB**: modello da utilizzare per documentare una violazione di dati personali e notificarla al garante
2	**Registro delle violazioni**: registro su cui memorizzare le violazioni avvenute.

10. DIAGRAMMA DI FLUSSO DELLE ATTIVITA' (



Allegato 1 – Modello DB

VIOLAZIONE DI DATI PERSONALI

MODELLO DI COMUNICAZIONE AL GARANTE

Secondo quanto prescritto dal Provvedimento del 2 luglio 2015, le amministrazioni pubbliche sono tenute a comunicare al Garante all'indirizzo: databreach.pa@pec.gpdp.it le violazioni dei dati personali (data breach) che si verificano nell'ambito delle banche dati (qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti, art. 4, comma 1, lett. p del Codice) di cui sono titolari.

La comunicazione deve essere effettuata entro 48 ore dalla conoscenza del fatto, compilando il modulo che segue.

Amministrazione titolare del trattamento:

Denominazione o ragione sociale: Provincia di Ancona

Sede legale: Strada di Passo Varano, 19 A- 60131 Ancona (AN).

Nome della persona fisica addetta alla comunicazione	
Cognome della persona fisica addetta alla comunicazione	
Funzione rivestita	
Indirizzo PEC e/o EMAIL per eventuali comunicazioni	
Recapito telefonico per eventuali comunicazioni	
Eventuali Contatti (altre informazioni	

Denominazione della/e banca/banche dati oggetto di data breach e breve descrizione della violazione dei dati personali ivi trattati

Quando si è verificata la violazione dei dati personali trattati nell'ambito della banca dati?

- ☐ Il _____
- ☐ Tra il _____e il_____
- ☐ In un tempo non ancora determinato
- ☐ È possibile che sia ancora in corso

Dove è avvenuta la violazione dei dati? (Specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)

Modalità di esposizione al rischio

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:

Dispositivo oggetto della violazione

- ☐ Computer Rete
- ☐ Dispositivo mobile
- ☐ File o parte di un file
- ☐ Strumento di backup

- ☐ Documento cartaceo
- ☐ Altro:

Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione:

Quante persone sono state colpite dalla violazione dei dati personali trattati nell'ambito della banca dati?

- ☐ N. _____ persone
- ☐ Circa _____ persone
- ☐ Un numero (ancora) sconosciuto di persone

Che tipo di dati sono oggetto di violazione?

- ☐ Dati anagrafici/codice fiscale
- ☐ Dati di accesso e di identificazione (user name, password, customer ID, altro)
- ☐ Dati relativi a minori
- ☐ Dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale
- ☐ Dati personali idonei a rivelare lo stato di salute e la vita sessuale
- ☐ Dati giudiziari
- ☐ Copia per immagine su supporto informatico di documenti analogici
- ☐ Ancora sconosciuto
- ☐ Altro:

Livello di gravità della violazione dei dati personali trattati nell'ambito della banca dati (secondo le valutazioni del titolare)?

- ☐ Basso/trascurabile
- ☐ Medio
- ☐ Alto
- ☐ Molto alto

Misure tecniche e organizzative applicate ai dati oggetto di violazione

La violazione è stata comunicata anche agli interessati?

- ☐ Sì, è stata comunicata il_____
- ☐ No, perché _____

Qual è il contenuto della comunicazione resa agli interessati?

Quali misure tecnologiche e organizzative sono state assunte per contenere la violazione dei dati e prevenire simili violazioni future?

Allegato 2 – Registro delle violazioni

Registro delle violazioni di dati personali

Il registro raccoglie tutte le violazioni rilevate, comprese quelle che non comportano rischi per i diritti e le libertà delle persone fisiche.

Banca dati violata	Data o periodo	Luogo della violazione	Modalità di esposizione del rischio	Sistemi coinvolti	Persone colpite	Tipi di dati	Livello di gravità	Misure a tutela dei dati	Misure a contrasto della violazione