COMUNE DI PONTE DI PIAVE

QUESTIONARIO DI VALUTAZIONE DELLA VIOLAZIONE DI DATI PERSONALI

Che cosa è avvenuto?
Descrivere l'incidente di sicurezza (es., divulgazione accidentale non autorizzata; perdita, distruzione; furto, attacco informatico)

Quando è accadutol'incidente?
Fornire informazioni sulla tempistica dell'incidente (es., accesso non autorizzato avvenuto il giorno 2 Feb 2019 alle ore 2:00 del mattino)

Quali categorie di dati sono state oggetto di incidente?
Indicare le tipologie di dati oggetto della violazione (es., dati biografici (nome,cognome) e dettagli di contatto (email))

Quanti Soggetti Interessati sono coinvolti dalla violazione?
Indicare il numero approssimativo di Soggetti Interessati i cui dati sono stati violati. (es., 1000)

Quali categorie di Soggetti Interessati sono coinvolti dalla violazione?
Indicare le categorie di Soggetti Interessati (es., dipendenti del Comune, consiglieri comunali, specifiche categorie di utenti)

L'incidente di sicurezza coinvolge altri Paesi EU o extra EU?
Indicare se vi sono altri Paesi esteri coinvolti (es., domiciliati esteri in Francia, in Svizzera,ecc)

Vi sono stati casi simili in passato? Se sì, descrivere la situazione già successa
(es., nel 2017 il Comune è stato oggetto di attacco informatico avvenuto ...)

Quali sistemi / dispositivi / strumenti sono stati oggetto di incidente?
Indicare i sistemi coinvolti dalla violazione di dati (es., workstation, smartphone, chiavette USB, etc.)

Quali misure tecniche e organizzative di sicurezza erano attive al momento dell'incidente?
Descrivere le misure di sicurezza in essere al momento della violazione (es., user ID e password complesse per accesso ai dati, log degli accessi al DB oggetto di attacco, crittografia del DB, DB in cloud presso il fornitore ... etc).

Sono coinvolti Responsabili esterni del trattamento?
Se sì, indicare il Responsabile del trattamento dei dati oggetto di violazione (es., fornitore ...).

Quali tipi di rischi /danni potrebbero incorrere i Soggetti Interessati dalla violazione?
Fornire informazioni sui rischi della violazione avvenuta e quali danni potrebbero essere / sono riscontrati per i Soggetti Interessati. (es., la perdita delle user ID e password degli utenti che usano la PEC fornita dal Comune potrebbe comportare l'accesso a comunicazioni riservate dell'utente; altri rischi finanziari, di reputazione).

Quali iniziative sono state prese per ridurre o eliminare il rischio attuale e l'ipotesi che si possa ripetere in futuro?
Se vi sono iniziative in corso e/o future per ridurre il disagio dell'incidente avvenuto ed evitare

che si ripeta, descrivere le misure contingenti e/o pianificate (es., le vulnerabilità del sistema sono state rimosse; la password è stata rafforzata come complessità; è pianificata una revisione di tutte le utenze entro il giorno ..., etc.).

E' possibile il ripetersi della violazione?
Descrivere le condizioni per cui potrebbe ripetersi la violazione (es., Si, il piano di rimedio delle vulnerabilità riscontrate richiede un tempo di 6 mesi; è stata data priorità alle misure ... per mitigare incidenti futuri).

FORNITORE CHE AGISCE COME RESPONSABILE DEL TRATTAMENTO DI DATI

Sono formalizzati livelli di servizio relativamente alla gestione dei dati e nel caso di incidente di sicurezza?
Se sì, descrivere gli accordi sulla gestione dei dati tra il Comune e il fornitore, anche per la gestione di violazioni di dati personali.

Che tipo di supporto ha fornito il responsabile esterno in merito all'incidente di sicurezza?
Fornire informazioni circa la tempistica di comunicazione del Data Breach e le iniziative svolte e/ o concordate con il Titolare in merito alla gestione della violazione di dati personali.