



<div><div><div>Città di Busca</div></div><div><div>Municipio di Valmala</div></div></div>	MODELLO ORGANIZZATIVO PROTEZIONE DEI DATI PERSONALI			
	Procedura di segnalazione interna di avvenuto data breach		Edizione 01 Revisione 00	Pag. 1
06-BRE		<i>N° di pagine</i> 4	<i>13.12.2021</i>	

Al personale designato

OGGETTO: SCHEDA INTERNA DI SEGNALAZIONE AVVENUTA VIOLAZIONE DEI DATI PERSONALI



Premesso che ai sensi dell'art. 33 del GDPR 2016/679 **“Notifica di una violazione dei dati personali all'autorità di controllo”**, in caso di violazione dei dati personali (in seguito “data breach”), il titolare del trattamento notifica la violazione all'autorità di controllo competente 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 dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche e che qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo;

si invita il personale designato a segnalare tempestivamente tutti i fatti che possano implicare una violazione di dati personali compilando ed inviando la presente scheda ai contatti indicati in calce alla presente.

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

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

- ☐ Il __/__/__, alle ore __, __
- ☐ Tra il __/__/__ e il __/__/__
- ☐ In un tempo non ancora determinato
- ☐ È possibile che sia ancora in corso

<div><div><div>Città di Busca</div><div></div></div><div><div>Municipio di Valmala</div><div></div></div></div>	MODELLO ORGANIZZATIVO PROTEZIONE DEI DATI PERSONALI		Edizione 01 Revisione 00		Pag. 2
	Procedura di segnalazione interna di avvenuto data breach				
	06-BRE		N° di pagine 4	13.12.2021	

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

4. 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 (specificare): _____


- Dispositivo oggetto della violazione

- ☐ Computer (specificare) _____
- ☐ Rete (specificare) _____
- ☐ Dispositivo mobile (specificare) _____
- ☐ File o parte di un file (specificare) _____
- ☐ Strumento di *backup* (specificare) _____
- ☐ Documento cartaceo (specificare) _____
- ☐ Altro (specificare): _____

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 _____

	MODELLO ORGANIZZATIVO PROTEZIONE DEI DATI PERSONALI		
	Procedura di segnalazione interna di avvenuto data breach		Edizione 01 Revisione 00
			Pag. 3
06-BRE		N° di pagine 4	13.12.2021

☐ 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/o la vita sessuale
- ☐ Dati giudiziari
- ☐ Copia per immagine su supporto informatico di documenti analogici
- ☐ Ancora sconosciuto
- ☐ Altro (specificare): _____


5. 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

6. Quali misure di sicurezza (tecniche e organizzative) erano state applicate ai dati oggetto di violazione?

7. La violazione è stata comunicata anche agli interessati?

- ☐ Sì, è stata fatta comunicazione in data __/__/__
- ☐ No, perché _____

	MODELLO ORGANIZZATIVO PROTEZIONE DEI DATI PERSONALI		
	Procedura di segnalazione interna di avvenuto data breach		Edizione 01 Revisione 00
			Pag. 4
06-BRE		N° di pagine 4	13.12.2021

8. (se alla domanda 7 è stato risposto Sì) Qual è il contenuto della comunicazione resa agli interessati?

9. Quali misure tecnologiche e organizzative sono state assunte per contenere la violazione dei dati?

10. Questa scheda è stata compilata da _____

Dati di contatto del Titolare del trattamento

Comune di Busca, Via Cavour 28 - 12022 Busca (CN), P.I. 00371290040 - C.F. 80003910041, PEC comune.busca@legalmail.it

Dati di contatto dell'Amministratore di Sistema (ADS)

Dott. Silvio ARMANDO
silvioarmando@comune.busca.cn.it

Dati di contatto del Responsabile della Protezione dei Dati (RPD)

Il RESPONSABILE DELLA PROTEZIONE DEI DATI (RPD) è l'AMBIENTE SICURO SERVIZI Società Cooperativa, Via Cascina Colombaro N. 56, 12100 Cuneo, Telefono 0171 451725 Fax 0171 451734, Email dpo@aesseservizi.eu Pec segreteria@pec.aesseservizi.eu.