MODULO DI SEGNALAZIONE DELLA VIOLAZIONE

Compilazione a cura di: **Operatore dell'Ente**

DATA EVENTO	
DATA	
ORA	
DATI DEL SEGNALATORE	
NOMINATIVO	
EMAIL	
TELEFONO	

Da tabella "Evento rilevato", selezionare l'evento che si è verificato. Se non presente descriverlo nella riga apposita in fondo della tabella.

In ogni caso circostanziare l'accadimento rilevato con una breve descrizione (ultima sezione del modello, **compilazione obbligatoria**).

EVENTO RILEVATO			
	CODICE EVENTO[1]	**EVENTO**	**DESCRIZIONE BREVE**
☐	**E1**	Abbandono della postazione di lavoro senza precauzioni	Un operatore abbandona la propria postazione di lavoro senza prima prendere le opportune precauzioni (riporre la documentazione, lasciare attive procedure sulla risorsa informatica utilizzata, ecc..) e terze persone possono

[1] Si tratta del codice numerico che identifica la tipologia di evento rilevato, da riportare sul Mod. DB02

			prendere visione di informazioni.
☐	**E2**	Account Amministratore compromesso	Il profilo dell'amministratore di sistema o comunque il profilo di un utente con privilegi elevati risulta compromesso.
☐	**E3**	Analisi e studio del sistema informatico da parte di terzi, con lo scopo di una possibile futura intrusione	Sono stati rilevati tentativi d'esame ed analisi del sistema informatico, con elevata probabilità che siano stati effettuati al fine di trovarne punti deboli e falle di sicurezza.
☐	**E4**	Blocco del servizio a causa di un attacco informatico (Denial of service)	Non è stato possibile accedere al sistema a causa di un attacco informatico di tipo D.o.S. (Denial of Service), che ha impedito il regolare svolgimento del servizio saturandone ed esaurendone le risorse. I dati presenti non sono stati alterati, ma l'accesso ai medesimi è stato bloccato per un tempo sufficiente a creare disagi.
☐	**E5**	Dati provenienti dal proprio sistema sono stati utilizzati per compiere una truffa	Dati provenienti dal proprio sistema sono stati impiegati per l'invio di comunicazioni a scopo di truffa o diffusione di false notizie. Per compiere tale tipo di illeciti sono state utilizzate informazioni appartenenti soltanto a questa struttura; ciò potrebbe indicare una compromissione, un accesso illecito o un utilizzo improprio del sistema o dei dati in esso contenuti.
☐	**E6**	Divulgazione non autorizzata di dati	Diffusione o comunicazione di dati, resi accessibili a destinatari non autorizzati, non indicati nel registro dei trattamenti o comunque fuori dalle liceità di trattamento.
☐	**E7**	E-mail invita a destinatari errati	Una o più e-mail contenenti dati personali sono state inviate a destinatari non autorizzati ad accedere a tali dati.
☐	**E8**	Furto di dati presenti in un archivio	I dati all'interno di uno o più archivi risultano rubati o copiati illegalmente.
	E9	Intrusione nel sistema con compromissione della riservatezza dei dati	Accesso abusivo al sistema da parte di terzi che ha portato ad una compromissione della riservatezza dei dati che vi erano all'interno.

☐			
☐	**E10**	Modifica di dati in modo errato e scorretto	Alcuni dati sono stati chiaramente alterati in modo scorretto rispetto alle loro versioni precedenti.
☐	**E11**	Modifica illecita del sito web, sfigurandolo e danneggiandolo con l'inserimento di immagini o testi inappropriati (Dafacement)	Il sito web è stato compromesso ed alterato nei suoi contenuti.
☐	**E12**	Perdita o danneggiamento di un archivio	Uno o più archivi fisici e/o digitali contenenti dati personali sono stati danneggiati o perduti.
☐	**E13**	Profilo utente compromesso, con possibile danneggiamento dei dati presenti	Il profilo di uno o più utenti è stato compromesso.
☐	**E14**	Ransomware / Cryptolocker	I dati di uno o più archivi informatici sono stati criptati in modo reversibile solamente tramite pagamento di un 'riscatto'.
☐	**E15**	Sfruttamento di una vulnerabilità tecnica del sistema per accedere, modificare o eliminare dati personali senza permesso	La presenza di una vulnerabilità tecnica all'interno del sistema informatico ha permesso l'accesso, la modifica o la cancellazione di dati personali in modo non autorizzato.
☐	**E16**	Truffa di dati personali avvenuta su internet attraverso l'inganno degli utenti (Phishing)	Uno o più utenti sono indotti, tramite inganno, a rivelare informazioni confidenziali ad individui e/o organizzazioni non autorizzate al trattamento.

☐	**E17**	Utilizzo improprio del sistema	Il sistema di gestione dei dati personali è stato utilizzato in modo improprio, trattando le informazioni in disaccordo a quanto descritto dall'Art.5, paragrafo 1, del Regolamento EU 2016/679. I principi descritti in tale articolo fanno riferimento alla "Liceità, Correttezza e Trasparenza" dei trattamenti, alle condizioni di limitazione delle finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, ed integrità e riservatezza.
☐	**E18**	Virus / trojan / Codice malevolo	Sottrazione, perdita d'accesso, alterazione e/o diffusione di dati personali dovuti all'utilizzo di codice malevolo (quale virus o trojan).
☐	**E19**	ALTRO (Descrivere evento)	

DESCRIZIONE EVENTO (Compilazione obbligatoria)