Allegato D.3)

REGISTRO DELLE VIOLAZIONI DI DATI PERSONALI													
Numero progressivo	Data di accadimento della violazione dati personali	Fonte e data della segnalazione	Natura della violazione (1)	Tipo di violazione (2)	Dispositivi interessati (3)	Dati personali interessati (4)	Effetti e conseguenze della violazione (5)	Misure tecniche e organizzative applicate (6)	Misure tecniche e organizzative adottate per contenere o annullare gli effetti della violazione o per prevenire violazioni future	Livello di gravità del rischio (7)	Notifica effettuata (8)	Comunicazione effettuata (9)	Note

(1) Accidentale o illecita

(2) - 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 sono in possesso dell'autore della violazione)
- Furto (i dati non sono più sui sistemi del Titolare e li ha l'autore della violazione)
- Accesso illegittimo
- Altro_____

(3) - Postazioni di lavoro
- Dispositivo di acquisizione o dispositivo-lettore
- Smart card o analogo supporto portatile
- File o parte di un file
- Strumento di back up
- Rete
- Altro_____

(4) - Dati anagrafici
- Numero di telefono
- Indirizzo di posta elettronica
- Dati di accesso e identificazione (username, password, altro)
- Dati personali (sesso, data di nascità, età, altro)
- Categorie particolari di dati personali art. 9 RGPD: dati ……..
- Dati relativi a condanne penali o reati art. 10 RGPD
- Dati sconosciuti
- Altro_____

(5) - Discriminazioni

- Furto o usurpazione di identità
- Perdite finanziarie
- Pregiudizio alla reputazione
- Perdita di riservatezza dei dati personali protetti da segreto professionale
- Perdita dell'esercizio del controllo sui dati personali
- Decifratura non autorizzata della pseudonimizzazione

(6) - Pseudonimizzazione e cifratura dati personali
- Assicurazione su base permanente della riservatezza, dell'integrità, della disponibilità e della resilienza dei sistemi e dei servizi di trattamento
- Ripristino tempestivo della disponibilità e dell'accesso ai dati personali in caso di incidente fisico o tecnico
- Verifica e valutazione sistematica dell'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento
- Limitazione della quantità di dati acquisiti (principio di minimizzazione)
- Chiavi robuste di autenticazione
- Idonei controlli sugli accessi
- Back up sicuri

(7) - Basso
- Medio
- Alto

(8) - Sì/No

(9) - Sì/No