**ALLEGATO 1**

**Intestazione dell’Istituto**

|  |
| --- |
| **REGISTRO INCIDENTI INFORMATICI** |
|  |
| **Numero Incidente**  | **2020/0001** |
|  |
| **A. Rilevazione dell’incidente** |
|   |
| Data e ora dell’incidente |  |
| Chi ha rilevato per primo l’incidente? Nominativo e riferimenti  |  |
| Data e ora di avvio della gestione dell’incidente |  |
| Note e/o breve descrizione dell’incidente |  |
| **B. Descrizione dell’incidente** |
|   |
| Origine dell’incidente (interna o esterna). Dettagliare bene l’origine |  |
| Sistemi e/o Applicazioni interessati dall’incidente  |  |
| Causa dell’incidente (se più cause indicare la prevalente) |  |
| Stato attuale (situazione diagnosticata) |  |
| Tempi previsti per la soluzione |  |
| Note |  |
| **C. Caratterizzazione dell’incidente** |
|  |
| Tipo Incidente (virus, attacco, alterazione dati, guasto apparati, sottrazione informazioni, blocchi, malfunzionamenti, ecc.)  |  |  |
| Sistemi colpiti e/o applicazioni colpite |  |  |
| Funzioni aziendali colpite |  |  |
| L’entità dell’incidente è tale da farlo rientrare nell’attenzione GDPR? SI/NO |  |  |
| Numero Clienti/Utenti oppure Numero Dipendenti colpiti dall’incidente (perdita e/o alterazione dati), ecc..  |  |  |
| Tipologia di dati coinvolti |  |  |
| Tipologia di soggetti coinvolti |  |  |
| Note |  |  |
|  |  |
| **D. Risoluzione dell’incidente** |  |
|  |  |
| Misure tampone intraprese nell’immediato |  |  |
| Ulteriori misure pianificate per la chiusura dell'incidente o poste in essere per evitare il ripetersi dell’incidente |  |  |
| Sono state allertate le strutture deputate ad attivare le eventuali comunicazioni GDPR? SI/NO  |  |  |
| Se SI, quando? (Data e Ora) |  |  |
| Se NO, spiegare le motivazioni di mancata comunicazione  |  |  |
| Chiusura incidente (Data e Ora) |  |  |
| Note |   |  |

**ALLEGATO 2**

**COMUNICAZIONE DI DATA BREACH AL GARANTE PRIVACY**

1. Titolare del trattamento

Ragione sociale/Nome e Cognome: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

C.F./P.IVA: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Stato: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

CAP: \_\_\_\_\_\_\_\_\_\_\_\_ Città: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Provincia: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Telefono: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Email: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

PEC: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Responsabile della protezione dei dati (o nel caso in cui non sia presente il RPD, i riferimenti di un altro soggetto presso cui ottenere più informazioni)

Denominazione: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Telefono: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Cellulare: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Email: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

PEC: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Quando si è verificata la violazione di dati personali?
* Il \_\_\_\_\_\_\_\_\_\_\_\_
* Tra il \_\_\_\_\_\_\_\_\_ e il \_\_\_\_\_\_\_\_\_\_\_\_
* In un tempo non ancora determinato
* È possibile che sia ancora in corso
1. Dove è avvenuta la violazione dei dati? (Specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)

|  |
| --- |
|  |

1. Modalità di esposizione al rischio

Tipo di violazione

* Lettura (presumibilmente i dati non sono stati copiati);
* Copia (i dati sono ancora presenti sul sistema 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).
1. Dispositivo oggetto della violazione
* Computer;
* Rete;
* Dispositivo mobile;
* File o parte di un file;
* Strumento di backup;
* Documento cartaceo;
* Altro (specificare).
1. Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione

|  |
| --- |
|  |

1. Quali sono le possibili conseguenze derivanti dalla violazione?

|  |
| --- |
|  |

1. Indicare le categorie di interessati colpiti dalla violazione

|  |
| --- |
|  |

1. Quante persone sono state colpite dalla violazione dei dati personali?
* n. \_\_\_\_\_ persone;
* circa \_\_\_\_\_ persone;
* un numero ancora sconosciuto di persone.
1. Numerosità dei dati di cui si presume la violazione

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Che tipo di dati sono oggetto di violazione?
* Dati anagrafici;
* Indirizzo di posta elettronica;
* Numero di telefono;
* Dati di accesso e di identificazione (user name, password, customer ID, altro);
* Dati relativi a minori;
* Dati particolari di cui all’art. 9 Reg. UE 2016/679;
* Dati giudiziari;
* Copia per immagine su supporto informatico di documenti analogici;
* Ancora sconosciuto;
* Altro (specificare).
1. Livello di gravità della violazione dei dati personali (secondo la valutazione del titolare)
* Basso/trascurabile;
* Medio;
* Alto;
* Molto alto.
1. Misure tecniche e organizzative applicate ai dati oggetto di violazione

|  |
| --- |
|  |

1. La violazione è stata comunicata anche agli interessati?
* Si, è stata comunicata in data \_\_\_\_\_\_\_\_\_;
* No, perché \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
1. Qual è il contenuto della comunicazione resa agli interessati?

|  |
| --- |
|  |

1. Quale canale è stato utilizzato per la comunicazione agli interessati?
2. La violazione coinvolge interessati che si trovano in altri Paesi UE?
* Sì;
* No.
1. La comunicazione è stata effettuata alle competenti autorità di altri Paesi UE?
* Sì (specificare quali);
* No.
1. Quali misure tecnologiche e organizzative sono state assunte per contenere la violazione di dati e prevenire simili violazioni future?

|  |
| --- |
|  |

Il Titolare del Trattamento

Dirigente Scolastico