|  |  |
| --- | --- |
| **SCHEDA EVENTO** | |
|  |  |
| Data della violazione anche solo presunta (specificando se è presunta) (1) |  |
| Data in cui si è avuto conoscenza della violazione |  |
| Modalità/fonte della segnalazione |  |
| Descrizione violazione |  |
| Natura della violazione (2) |  |
| Causa della violazione(3) |  |
| Tipologia di dati oggetto della violazione (4) |  |
| Volume (anche approssimativo) dati personali oggetto di violazione(5) |  |
| Dispositivo o supporto oggetto della violazione (6) |  |
| Descrizione dei sistemi e delle infrastrutture IT coinvolti nell’incidente e indicazione della relativa ubicazione |  |
| Numero interessati coinvolti (7) |  |
| Categorie di interessati coinvolti (8) |  |
| Misure di sicurezza tecniche e organizzative applicate ai dati, sistemi e infrastrutture IT coinvolti (9) |  |
| Descrizione delle probabili conseguenze |  |
| Valutazione livello gravità della violazione (secondo il Responsabile)(10) |  |
| Misure tecniche e organizzative per porre rimedio alla violazione e contenerne gli i effetti negativi (11) |  |

|  |  |
| --- | --- |
| **Contratto/convenzione cui accede la nomina a Responsabile del trattamento** | |
| oggetto |  |
| data di stipula/scadenza |  |
| referente contratto (RES) per l’Azienda Usl Toscana sud est |  |

|  |  |
| --- | --- |
| **Dati di contatto del Responsabile del trattamento** | |
| Responsabile del trattamento |  |
| Codice Fiscale/Partita Iva |  |
| Stato |  |
| Indirizzo |  |
| Città |  |
| CAP |  |
| Telefono |  |
| E-mail |  |
| PEC |  |

|  |  |
| --- | --- |
| **Dati di contatto del Responsabile della Protezione dei Dati (RPD)** | |
| nome |  |
| cognome |  |
| Telefono |  |
| E-mail |  |
| PEC |  |

|  |  |
| --- | --- |
| **Altro punto di contatto del Responsabile per ulteriori informazioni** | |
| nome |  |
| cognome |  |
| Telefono |  |
| E-mail |  |
| PEC |  |

Luogo e data……………………………………………………………………..

p. il Responsabile del trattamento il Rappresentante legale

……………………………………………………………………………………………

(1) Il … / Dal … (violazione ancora in corso) / Dal … al …/ In un tempo non ancora determinato.

(2) diffusione/acceso non autorizzato o accidentale modific non autorizzata o accidentale, impossibilità di accesso, perdita, distruzione non autorizzata o accidentale

(3) Azione intenzionale interna / azione accidentale interna / azione intenzionale esterna / azione accidentale esterna / sconosciuta / altro (specificare)

(4) Dati anagrafici (nome, cognome, sesso, data di nascita, luogo di nascita, codice fiscale, altro...) / dati di contatto (indirizzo postale o di posta elettronica, numero di telefono fisso o mobile) / dati di accesso e di identificazione (username, password, customer id, altro…) / dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro…) / dati relativi alla fornitura di un servizio di comunicazione elettronica (dati di traffico, dati relativi alla navigazione internet, altro…) / dati relativi a condanne penali e ai reati o a connesse misure di sicurezza o di prevenzione / dati di profilazione / dati relativi a documenti di identificazione/riconoscimento (carta di identità, passaporto, patente, CNS, altro…) / dati di localizzazione / dati che rivelino l’origine razziale o etnica / dati che rivelino opinioni politiche / dati che rivelino convinzioni religiose o filosofiche / dati che rivelino l’appartenenza sindacale / dati relativi alla vita sessuale o all’orientamento sessuale / dati relativi alla salute / dati genetici / dati biometrici / altro (specificare).

(5)N………Circa n…………Un numero (ancora ) non definito di dati

(6) Banca dati elettronica / personal computer / dispositivo di acquisizione o dispositivo-lettore / smart card o analogo supporto portatile / file o parte di un file / strumento di back up / rete / documento cartaceo / altro (specificare)

(7)Indicare il numero preciso oppure quello stimato oppure che il numero è ancora sconosciuto

(8)Dipendenti / collaboratori / contraenti / pazienti /minori /persone vulnerabili(altro (specificare)

(9) Indicare le misure in essere al momento della violazione (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/altro (specificare))

(10)Trascurabile/basso/medio/alto

(11) Distinguere tra misure adottate e misure in corso di adozione