

## Procedura “Gestione delle Violazioni di Dati Personali” – Allegato 2

### Tipologia di eventi

#### Tipologia di eventi

Di seguito si riportano le tipologie di eventi che possono generare una Violazione dei dati personali, di cui si fornisce di seguito una tassonomia.

Tipologia di eventi	Descrizione
<b>Eventi accidentali nei trattamenti elettronici dei dati</b>	Eventi anomali determinati da casi fortuiti o comportamenti colposi nell'ambito dei trattamenti informatizzati, effettuati sui dati personali gestiti dall'Organizzazione. Possono generarsi nell'ambito delle attività di gestione nei sistemi e delle infrastrutture IT sia svolte internamente che esternalizzate a terzi. I motivi possono essere molteplici e tra questi si evidenziano le errate configurazioni dei sistemi e dei PC, la mancata o errata applicazione di policy o procedure di sicurezza, la distrazione e/o esecuzione erranea di operazioni, l'esaurimento del ciclo di vita delle componenti hardware, il danneggiamento delle componenti hardware, i malfunzionamenti software, la comunicazione o diffusione erronee di dati a soggetti non autorizzati, l'interruzione di servizi informatici, la modifica erranea di informazioni, basi di dati, archivi, autorizzazioni all'accesso, ecc...
<b>Eventi accidentali nei trattamenti cartacei dei dati</b>	Eventi anomali determinati da casi fortuiti o comportamenti colposi nell'ambito dei trattamenti non automatizzati effettuati sugli archivi cartacei di dati personali dell'Organizzazione. Tra questi si evidenziano lo smarrimento o distruzione accidentale di documenti (es. incendio, allagamento locali, ecc), la comunicazione o diffusione erronee di dati a soggetti non autorizzati, la modifica erranea, il mancato aggiornamento dei dati, ecc...
<b>Eventi dolosi</b>	Comportamenti dolosi da parte di personale interno o soggetti esterni, anche per finalità di frode, sfruttando un accesso legittimo ai dati, ai sistemi ed agli archivi cartacei, oppure mediante accesso non autorizzato ai dati attraverso il furto di credenziali o dispositivi, lo sfruttamento di vulnerabilità presenti sui sistemi, la compromissione di credenziali di autenticazione, l'utilizzo di software malevolo oppure effettuando comportamenti dolosi nell'ambito di trattamenti cartacei. Tali eventi possono includere i furti di supporti di archiviazione/elaborazione contenenti dati personali (es. furto di PC portatili, hard disk, chiavette USB, smartphone, tablet, ecc.) ed il furto di documenti cartacei.