GUIDA PER LA VALUTAZIONE DELLE VIOLAZIONI

CODICE EVENTO	TITOLO	DESCRIZIONE EVENTO	VALUTAZIONI DA FARE	CLASSIFICAZIONE	RISCHIO
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 prendere visione di informazioni.	E' importante individuare la tipologia di informazioni a cui terzi non autorizzati potrebbero aver avuto accesso.	Accesso non autorizzato – Accidentale	MEDIO
E2	**Account Amministratore compromesso**	Il profilo dell'Amministratore di Sistema o comunque il profilo di un utente con privilegi elevati risulta compromesso.	Tutti i dati accessibili devono essere considerati compromessi e alterati. La probabile riprogettazione del sistema (o di buona parte di esso) e della sua sicurezza è da considerarsi fortemente consigliata.	Modifica non autorizzata – Compromissione	ALTO
E3	**Aggiornamento archivio non riuscito**	Un aggiornamento delle informazioni, per disguido tecnico determina all'interno di una base dati la perdita dei collegamenti a determinate informazioni (accidentale)	Sarà importante individuare il disguido tecnico.	Modifica non autorizzata – Accidentale	MEDIO
E4	**Analisi e studio del sistema informatico da parte di terzi, con lo scopo di una possibile futura intrusione**	Sono stati rilevati tentativi d'esame e analisi del sistema informatico, con l'alta possibilità che siano stati effettuati al fine di trovarne punti deboli e falle di sicurezza.	Questa pratica non va sottovalutata, molto spesso sta ad indicare un tentativo di intrusione all'interno del sistema. È quindi essenziale intervenire al più presto per impedirne lo svolgimento.	Accesso non autorizzato – Spionaggio	ALTO
E5	**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.	Sarà importante svolgere indagini per individuare la provenienza dell'attacco informatico e con quali tecniche.	Accesso non autorizzato – Spionaggio Perdita di accesso – Ransomware	ALTO
E6	**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.	Sarà importante svolgere indagini più approfondite e mettere in atto delle azioni volte a migliorare la sicurezza.	Accesso non autorizzato – Spionaggio	ALTO
E7	**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.	La violazione è tale indipendentemente dalla quantità di record e destinatari coinvolti. È però essenziale fare un'attenta valutazione d'impatto dell'evento e del reale danno arrecato.	Divulgazione non autorizzata – Infoting	MEDIO
E8	**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.	Le informazioni presenti all'interno di queste e-mail sono da considerarsi diffuse, indipendentemente dalla gravità dell'evento. I provvedimenti più adeguati da adottare saranno poi determinati in relazione al tipo di dati divulgati. Potrebbe ad esempio essere doveroso avvisare i soggetti interessati dell'accaduto e/o stabilire una formazione aggiuntiva per gli autori di tale violazione (a titolo precauzionale), questo per aumentare la consapevolezza interna in termini di sicurezza e di strumenti utilizzati.	Divulgazione non autorizzata – Accidentale	MEDIO
E9	**Furto di dati presenti in un archivio**	I dati all'interno di uno o più archivi risultano rubati o copiati illegalmente.	Avvisare i soggetti interessati dell'incidente e, se necessario, l'autorità competente. Importante è anche valutare attentamente se i diritti e le libertà degli interessati sono stati violati, con il rischio di aver causato un danno ai medesimi.	Copia non autorizzata – Furto	ALTO
E10	**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.	Se non vi sono evidenti prove, inoltre, non si può essere certi di un danneggiamento all'integrità dei dati trattati, ma non si deve neppure escluderne la possibilità. È quindi necessario portare avanti delle indagini per scoprire le modalità di accesso e l'eventuale danno ai dati. Fino a quando non si avranno delle risposte sicure, ogni dato del sistema è da considerarsi possibilmente modificato.	Accesso non autorizzato – Spionaggio	ALTO
E11	**Modifica di dati in modo errato e scorretto**	Alcuni dati sono stati chiaramente alterati in modo scorretto rispetto alle loro versioni precedenti.	Questo evento potrebbe indicare, ad esempio, un accesso non autorizzato alle informazioni o la presenza, nel gruppo di lavoro, di un operatore con una formazione carente. Individuare la causa di questa modifica assume quindi un'importanza primaria al fine di fermare o mitigare l'evento. Utilizzare le copie dei backup precedenti potrebbe essere un ottimo modo per recuperare e verificare i dati corretti.	Modifica non autorizzata – Accidentale	BASSO
E12	**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.	Non si possono perciò ritenere valide e attendibili le informazioni al suo interno. Inoltre, sono da considerarsi compromessi e inaffidabili anche eventuali dati inseriti o recuperati on-line successivamente alla modifica. La manipolazione della pagina, infatti, potrebbe aver coinvolto anche la logica e le comunicazioni da e verso il sito, rendendo superfluo un tentativo di recupero del sito originario.	Modifica non autorizzata – Compromissione	ALTO
E13	**Perdita o danneggiamento di un archivio**	Uno o più archivi fisici e/o digitali contenenti dati personali sono stati danneggiati o perduti.	In caso di distruzione il danno si limita alla perdita d'accesso alle informazioni, eventualmente recuperabile tramite backup e copie di sicurezza. In caso di perdita, invece, bisogna considerare la possibilità di ritrovamento ed accesso da parte di terzi non autorizzati, con conseguente utilizzo o divulgazione dei dati contenuti. Per determinare la gravità dell'evento è necessaria un'attenta valutazione della tipologia dei dati coinvolti nella violazione.	Accesso non autorizzato – Accidentale	MEDIO
E14	**Profilo utente compromesso, con possibile danneggiamento dei dati presenti**	Il profilo di uno o più utenti è stato compromesso.	Tutti i dati relativi ai profili coinvolti sono da considerarsi incompleti e non più affidabili. Se il soggetto danneggiato è un Amministratore di sistema, o un utente con privilegi molto elevati, è necessario mettere in atto un'opera sostanziale di recupero e messa in sicurezza dei dati. Se invece il soggetto risulta un operatore, è consigliabile un confronto con le copie di backup per verificare quali e quante sono state le effettive variazioni.	Modifica non autorizzata – Compromissione	ALTO
E15	**Ransomware / Cryptolocker**	I dati di uno o più archivi informatici sono stati criptati in modo reversibile solamente tramite pagamento di un 'riscatto'.	L'accesso a tali dati è precluso, Il recupero dei dati è ancora possibile tramite backup verificati se disponibili. Il recupero tramite pagamento di quanto richiesto NON E' garantito e soluzioni affidabili alternative sono da preferirsi ove possibile.	Perdita di accesso – Ransomware	ALTO

E16	**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.	È possibile un recupero dei dati utilizzando le copie non alterate dei backup, ed è inoltre suggerita la comunicazione dell'accaduto ai soggetti autorizzati ad accedere ai dati. L'utilizzo di tale debolezza del sistema DEVE essere bloccato al più presto per evitare ulteriori danni, e devono essere urgentemente messe in pratica azioni volte a prevenire questo genere di situazioni.	Accesso non autorizzato – Spionaggio Modifica non autorizzata – Compromissione Cancellazione – Distruzione	ALTO
E17	**Truffa di dati personali comuta 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.	Questa tipologia di truffa online è chiamata "Phishing" ed è comunemente svolta tramite e-mail o messaggi che apparentemente sono uguali a quelli di legittimi fornitori di servizi e chiedono al destinatario la comunicazione di dati precisi. Potrebbe essere utile un'identificazione della quantità e della tipologia dei dati rubati, per poter prendere decisioni adeguate sulla risoluzione del problema. Inoltre, dovrebbe essere migliorata o integrata la formazione degli operatori coinvolti, al fine di aumentare la sicurezza dei dati.	Divulgazione non autorizzata – Infoting	ALTO
E18	**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.	In questo caso, è raccomandato fare un controllo attento dei trattamenti, ponendo maggiormente attenzione a ciò che ci viene richiesto dal precedente articolo.	Accesso non autorizzato – Accidentale Copia non autorizzata – Accidentale Divulgazione non autorizzata – Accidentale	MEDIO
E19	**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).	Sono fortemente raccomandati: l'immediata rimozione di tale codice, il tempestivo avviso di quali e quanti dati sono stati colpiti ed il recupero di quelli non compromessi. Per evitare che possa verificarsi nuovamente, si consiglia di adottare una migliore politica di gestione del software e di mettere in pratica una formazione adeguata del personale, oltre ad un eventuale audit dei sistemi di intrusion prevention, antivirus ed antispam.	Copia non autorizzata – Furto Modifica non autorizzata – Compromissione Divulgazione non autorizzata – Infotin	ALTO