SCHEDA DI INCIDENTE DI SICUREZZA

A) ANALISI

ID	DESCRIZIONE	*Esempio*	INFORMAZIONI DI BASE	INFO DI DETTAGLIO / NOTE
1	**Data ed ora Evento** *(anche solo approssimativa o presunta; se presunta specificarlo nel campo Note)*	*1/6/2021, ore 17:15*		
2	**Data ed ora ricezione segnalazione** (*momento di presa di conoscenza dell'Evento)*	*15/6/2021, ore 09:25*		
3	**Luogo dell'Evento** (indirizzo)	*Sede di Via Cristoforo Colombo 25*		
4	**Supporti / sistemi di elaborazione e/o memorizzazione dei dati coinvolti** (con indicazione della loro ubicazione)	*Archivio cartaceo collocato nel seminterrato; data center dell'outsourcer XYZ sito in…..; server locale; NAS marca e modello (vedi elenco strumenti di trattamento)*		
5	**Canale di segnalazione**	*Orale, telefono, e-mail*		
6	**Fonte della segnalazione**	*Personale interno / soggetto interessato / fornitore esterno*		
7	**Come ci si è accorti dell'incidente?**	*Perché i file sul computer non erano più accessibili / perché abbiamo visto acqua nel seminterrato / ecc.*		

8	**Tipologia evento anomalo**	*Evento naturale; Evento intenzionale di origine umana; Evento non intenzionale di origine umana; Evento di carattere tecnico (vedi* MINACCE*)*		
9	**Descrizione evento anomalo**	*Attacco informatico, furto / smarrimento di dispositivo, incendio, allagamento …)*		
10	**Tipologia di documenti coinvolti**	*Documenti cartacei, file (testo, fogli di calcolo, immagini), ecc...*		
11	**Tipologia/e di persone coinvolte**	*Clienti/utenti, lavoratori, fornitori, pazienti, ecc… (elenco interessati)*		
12	**Numero di persone coinvolte** *(anche indicativo)* **per ciascuna categoria**	*Utenti: tra 100 e 200; lavoratori: 40;* OPPURE *attualmente sconosciuto / indeterminabile*		
13	**Tipologia/e di dati personali comuni coinvolti**	*Es. dati anagrafici e di contatto (indirizzo email, telefono) vedi elenco indicativo dati personali comuni) OPPURE NESSUNO*		
14	**Tipologia/e di dati personali particolari coinvolti**	*Dati relativi alla salute, dati biometrici (vedi elenco indicativo dati personali particolari) OPPURE NESSUNO*		
15	**Tipologia/e di altre informazioni coinvolte**	*progetti, piani commerciali, disegni, elenchi fornitori, policy di sicurezza, documenti contabili, documentazione comunque riservata (oppure NESSUNA)*		
16	**Misure di sicurezza fisiche perimetrali sui dati / informazioni coinvolti**	*vedi elenco indicativo misure di sicurezza fisiche perimetrali*		
17	**Misure di sicurezza informatiche sui dati / informazioni coinvolte**	*vedi elenco indicativo misure di sicurezza informatiche*		
15	**Misure di sicurezza organizzative sui dati / informazioni coinvolte**	*vedi elenco indicativo misure di sicurezza organizzative*		

16	**Tipologia/e di violazione** 1. *lettura (presumibilmente i dati non sono stati copiati)* 2. *copia (i dati sono ancora presenti sul sistema del titolare)* 3. *alterazione (i dati sono presenti sui sistemi ma sono stati alterati)* 4. *cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione)* 5. *furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione)* 6. *altro*	*I documenti contenenti i dati sono andati bruciati / i dati sono stati criptati da un ransomware*		
17	**Natura della violazione**	*Temporanea / Definitiva*		
18	**Rischi per le persone potenzialmente o effettivamente coinvolte**	*vedi elenco indicativo rischi per i diritti e le libertà*		
19	**Probabilità del/dei rischio/i**	*Non siamo in grado di valutare allo stato / Inesistente / Molto bassa / Bassa / Media / Alta / Molto Alta (indicare motivazione nelle note)*		
20	**Gravità del/dei rischio/i**[1]	*Non siamo in grado di valutare allo stato / Inesistente / Molto bassa / Bassa / Media / Alta / Molto Alta (indicare motivazione nelle note)*		
21	**Procedura gestione incidenti: è stata seguita?**	*Presente e osservata / Presente ma non osservata / Assente / Non siamo in grado di rispondere*		
22	**Soggetti esterni eventualmente a conoscenza dell'evento**	*Nessuno / Nessuno / potenzialmente chiunque, i dati sono pubblici / non ancora noto / impossibile stabilirlo*		
23	**Contestazioni/richieste da parte di terzi**	*No / Non ancora / Inapplicabile / chiesto riscatto di € ... (indicare motivazione nelle note)*		

1 Ai fini della conduzione di "Severity Assessment", si segnalano le seguenti risorse online, gratuite, basate sulla metodologia ENISA: https://www.projit.it/privacy_it/pdbseveritycalculator/story_html5.html - https://lt42.tech/databreach/severityassessment

24	**Danni**	*Nessuno / Non ancora manifestatisi / inapplicabile (indicare motivazione nelle note)*		
25	**Individuazione del responsabile dell'evento anomalo** *(indicare chi, senza il nome)*	*Sì / No / Non ancora / Non possibile Es. uno o più dipendenti ancora da individuare*		
26	**Denunce / esposti / querele all'autorità** *(in caso illecito di reato o sospetto tale)*	*Presentata / Non ancora presentata / Non applicabile perché non ci sono comportamenti penalisticamente rilevanti*		
27	**Azioni intraprese a seguito della conoscenza dell'evento per ridurre i rischi e/o limitare i danni**	*Nessuna / Cancellazione remota (remote wipe) del dispositivo sottratto*		
28	**Azioni pianificate per ridurre i rischi e accertare natura ed entità dei danni**	*Nessuna / incarico ad un informatico esterno per analisi forense dei sistemi attaccati / apertura sinistro verso assicurazione*		
29	**Azioni pianificabili per evitare il ripetersi dell'evento**	*Nessuna / stipula assicurazione contro i danni*		

ULTERIORI EVENTUALI OSSERVAZIONI

B) VALUTAZIONE[2]

1) L'Evento anomalo consiste effettivamente in una violazione di dati (indipendentemente dal livello di probabilità del rischio)**?**

SI' / NO	**MOTIVAZIONE / NOTE** *(es. falso positivo, in quanto …)*

2 Ad opera del Redattore e/o del Revisore della Scheda.

2) Quali adempimenti occorre eseguire?

ADEMPIMENTO	DA ESEGUIRE / NON NECESSARIO	MOTIVAZIONE / NOTE
Annotazione nel registro dei *data breach* (art. 33 § 5 GDPR)		
Notifica preliminare del *data breach* (Guidelines WP29 WP250rev.01, § II.B.2 - "*Notification in phases*")		
Notifica completa del *data breach* (art. 33 § 1 GDPR)		
Segnalazione al titolare del trattamento[3] (art. 33 § 2 GDPR)		
Comunicazione della violazione agli interessati (art. 34 GDPR)		
Segnalazione al cliente / fornitore[4]		

Riferimenti essenziali:

- Violazione dei dati personali (Data Breach)
- WP29 - Guidelines WP250rev.01
- EDPB - Guidelines 01/2021 on Examples regarding Data Breach Notification
- Home - Notifica di una violazione dei dati personali (data breach)
- Personal data breaches — ENISA

C) INFORMAZIONI CONCLUSIVE

	COGNOME/I E NOME/I	FUNZIONE / RUOLO	DATA	FIRMA/FIRME[5]
REDATTORE/I				

3 Applicabile solo quando l'organizzazione che compila la scheda opera come Data Processor (responsabile del trattamento) per conto di altre organizzazioni.
4 Applicabile nel caso in cui nell'incidente siano coinvolte informazioni riservate non costituenti dati personali.
5 *Ai fini dell'archiviazione dell'originale cartaceo della scheda compilata in ogni sua parte. E' possibile apporre anche firma digitale (formato PAdES preferibilmente).*

REVISORE/I				
VALIDATORE/I				