Casistica WP 29 in Italiano (fonte: Italia Oggi, 14 marzo 2018 serie speciale nr.5)

Casi	Notificare all'Autorità sdi Controllo	Comunicazione agli Interessati	Note
1. Un Titolare del Trattamento ha conservato copia di un archivio di dati personali criptati su un CD. Il CD viene rubato	No	No	Fino a che i dati vengono crittografati con un algoritmo avanzato, esistono backup dei dati e la chiave univoca non è compromessa, questa non è una violazione da segnalare. Tuttavia, se i dati vengono successivamente compromessi, è necessaria la notifica
2. Dati personali vengono esportati da un sito internet sicuro gestito dal titolare del trattamento durante un attacco informatico. Il titolare del trattamento ha clienti in un singolo Stato della Ue	Si, bisogna notificare l'Autorità di Controllo se ci sono potenziali conseguenze per i singoli interessati	Si, dipende dalla natura dei dati personali affetti e dalla gravità delle conseguenze per i singoli interessati	

Casi	Notificare all'Autorità sdi Controllo	Comunicazione agli Interessati	Note
3. Un breve black-out, della durata di alcuni minuti, impedisce il funzionamento dei call center del titolare del trattamento. Di conseguenza i clienti non possono accedere ai loro dati	No	No	Non si tratta di una violazione dei dat personali da segnalare, ma si tratta comunque di un incidente registrabile ai sensi dell'articolo 33(5). Appropriata registrazione devono essere conservati dal titolare del trattamento
4. Il titolare del trattamento subisce un attacco ransomware che provoca la crittografia di tutti i dati. Non sono disponibili back-up e i dati non possono essere ripristinati. Durante le indagini, diventa chiaro che l'unica funzionalità del ransomware era quella di crittografare i dati e che non vi erano altri malware presenti nel sistema	Sì, riferire all'autorità di vigilanza competente, se ci sono potenziali conseguenze per gli individui in quanto si tratta di una perdita di disponibilità di dati.	Sì, a seconda della natura dei dati personali interessati e del possibile effetto della mancanza di disponibilità dei dati, nonché di altre possibili conseguenze	Se fosse disponibile una copia di riserva e i dati potessero essere ripristinati in tempo utile, ciò non dovrebbe essere segnalato all'autorità di vigilanza o agli Interessati in quanto non vi sarebbe stata alcuna perdita permanente di disponibilità o riservatezza dei dati. Tuttavia, l'autorità di controllo può prendere in considerazione un'inchiesta per valutare la conformità ai requisiti di sicurezza dell'articolo 32
5. Un cliente telefona al call center di una banca per segnalare una violazione dei dati poiché ha ricevuto una dichiarazione mensile del conto bancario non proprio	Sì	Solo le persone interessate vengono avvisate se c'è un rischio elevato ed è chiaro che altri non sono stati colpiti	Se, dopo ulteriori indagini, viene identificato un numero maggiore di persone interessate, è necessario eseguire un aggiornamento dell'autorità di vigilanza e il controllore effettua il passaggio aggiuntivo per notificare agli altri individui se vi è un rischio elevato per loro

Il titolare del trattamento intraprende una breve indagine (completata entro 24 ore) e stabilisce con ragionevole certezza che si è verificata una violazione dei dati personali e se si tratta di un difetto sistemico che ha o potrebbe interessare altri clienti			
6. Un mercato online multinazionale subisce un attacco informatico e nomi utente, password e cronologia degli acquisti sono pubblicati online dall'autore dell'illecito	Sì, segnalare all'autorità di vigilanza capofila se comporta l'elaborazione transfrontaliera	Sì, già che ci possono essere conseguenti rischi	Il titolare del trattamento dovrebbe agire, ad es. forzando il ripristino della password degli account interessati, nonché altri passaggi per mitigare il rischio
7. Una società di hosting di siti web (responsabile del trattamento) identifica un errore nel codice che controlla l'autorizzazione dell'utente. Ciò implica che ogni utente possa accedere ai dettagli dell'account di qualsiasi altro utente	Come responsabile del trattamento, la società di hosting di siti Web deve informare i suoi clienti interessati (i titolari del trattamento) prontamente. Supponendo che la società di hosting abbia condotto la propria indagine, i titolari del trattamento interessati dovrebbero essere ragionevolmente fiduciosi sul fatto che tutti abbia subito una violazione e quindi è vengono considerati come "informati" una volta che sono stati notificati dalla società di hosting (responsabile del trattamento)	Se non ci sono alti rischi per i singoli interessati, essi non devono essere avvisati	La società di hosting del sito web (titolare del trattamento) deve prendere in considerazione qualsiasi altro obbligo di notifica (ad esempio ai sensi della direttiva NIS). Se non vi è alcuna prova che questa vulnerabilità sia sfruttata con questo particolare responsabile del trattamento, una violazione notificabile potrebbe non essersi verificata ma potrebbe essere registrabile o essere oggetto di non conformità ai sensi dell'articolo 32

Casi	Notificare all'Autorità sdi Controllo	Comunicazione agli Interessati	Note
	I titolari del trattamento devono quindi informare l'autorità di vigilanza		
8. Le cartelle cliniche di un ospedale non sono disponibili per un periodo di 30 ore a causa di un attacco informatico	Sì, l'ospedale è obbligato a notificare già che ci possono essere gravi conseguenze per il benessere del paziente e la sua privacy	Sì, comunicare alle persone colpite	
9. I dati personali di 5000 studenti vengono erroneamente inviati alla mailing list sbagliata con oltre 1000 destinatari	Sì, riferire all'autorità di vigilanza	Sì, comunicare gli interessati in base alla portata e al tipo di dati personali coinvolti e alla gravità delle possibili conseguenze	
10. Una e-mail di marketing diretto viene inviata ai destinatari nel campo "a:" o "cc:", consentendo in tal modo a ciascun destinatario di vedere l'indirizzo e-mail di altri destinatari	Sì, la notifica all'autorità di vigilanza può essere obbligatoria se un numero elevato di persone è interessato, se vengono rivelati dati sensibili (ad esempio una mailing list di uno psicoterapeuta) o se altri fattori presentano rischi elevati (ad esempio, la posta contiene password)	Sì, comunicare agli interessati in base alla portata e al tipo di dati personali coinvolti e alla gravità delle possibili conseguenze	La notifica potrebbe non essere necessaria se non vengono rivelati dati sensibili e se viene rivelato solo un numero minore di indirizzi e-mail