Allegato B

Data Breach response plan

(Regolamento (UE) 2016/679, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati)

Sommario

VERSIONI DEL DOCUMENTO		
EDIZIONE	**SINTESI DELLA MODIFICA**	**DATA**
1.0	Prima versione del documento	*<Data di adozione>*

1. SCOPO E CAMPO DI APPLICAZIONE

La presente procedura definisce le modalità operative, i compiti e le responsabilità relativi alla gestione delle violazioni di dati personali che potrebbero comportare un rischio per i diritti e le libertà delle persone fisiche (Data Breach).

2. RIFERIMENTI NORMATIVI

- Regolamento (UE) 2016/679, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (di seguito definito RGPD);
- Allegato 1 al Provvedimento del 2 luglio 2015 del Garante per la Protezione dei dati personali;
- Guidelines on Personal Data breach notification under Regulation 2016/679 fonte Article 29 Data Protection Working Party:
- Recommendations for a methodology of the assessment of severity of personal data breaches – ENISA.
- Provvedimento del Garante sulla notifica delle violazioni dei dati personali (data breach) - 30 luglio 2019 [9126951]

3. DEFINIZIONI

Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Titolare del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.

Referente del Titolare: il soggetto designato dal titolare per la gestione del processo di escalation del Data Breach all'interno dell'Ente; è identificato nel ruolo del Responsabile dell'area/settore in cui si è rilevato l'evento di sicurezza, per il contesto di propria competenza.

Responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

Violazione dei dati personali (*Personal Data Breach*): la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Responsabile per la Protezione dei Dati: è il soggetto individuato dal titolare ai sensi degli artt. 37-39 del Regolamento UE 2016/679, che ha compiti di controllo e di supporto alla struttura in tema di protezione dei dati personali

Autorità di Controllo: Autorità Garante per la protezione dei dati personali.

WP29: Gruppo di lavoro composto da un rappresentante delle autorità di protezione dei dati personali designate da ciascuno Stato membro dell'Unione Europea.

4. TIPOLOGIE DI VIOLAZIONI DI DATI PERSONALI

Le "*Guidelines on Personal data breach notification under Regulation 2016/679*" definiscono le seguenti tipologie di violazioni:

- "Confidentiality breach" - quando si verifica una violazione che comporti un accesso o una divulgazione accidentale o non autorizzata di dati personali.
- "Integrity breach" - quando si verifica una violazione che comporti una alterazione accidentale o non autorizzata di dati personali.
- "Availability breach" - quando si verifica una violazione che comporti la perdita di disponibilità o la distruzione accidentale o non autorizzata di dati personali.

5. LE POSSIBILI CONSEGUENZE DELLE VIOLAZIONI DI DATI PERSONALI

Una violazione può potenzialmente provocare una serie di effetti avversi significativi sugli individui, che possono causare danni fisici, materiali o immateriali. Il RGPD spiega che ciò può includere la perdita del controllo sui propri dati personali, la limitazione dei loro diritti, discriminazione, furto d'identità o frode, perdita finanziaria, inversione non autorizzata di pseudonimizzazione, danno alla reputazione e perdita di riservatezza dei dati personali protetti dal segreto professionale. Può anche includere qualsiasi altro significativo svantaggio economico o sociale per tali individui (*Cosiderandi 75 e 85 RGPD*).

Di conseguenza, il RGPD richiede che il titolare del trattamento notifichi una violazione all'autorità di vigilanza competente, a meno che non sia improbabile che possa comportare il rischio che tali effetti negativi si verifichino. Laddove vi sia un rischio probabile che si verifichino tali effetti avversi, il RGPD richiede che il titolare del trattamento comunichi la violazione agli individui interessati non appena sia ragionevolmente fattibile (*Considerando 86 RGDP*).

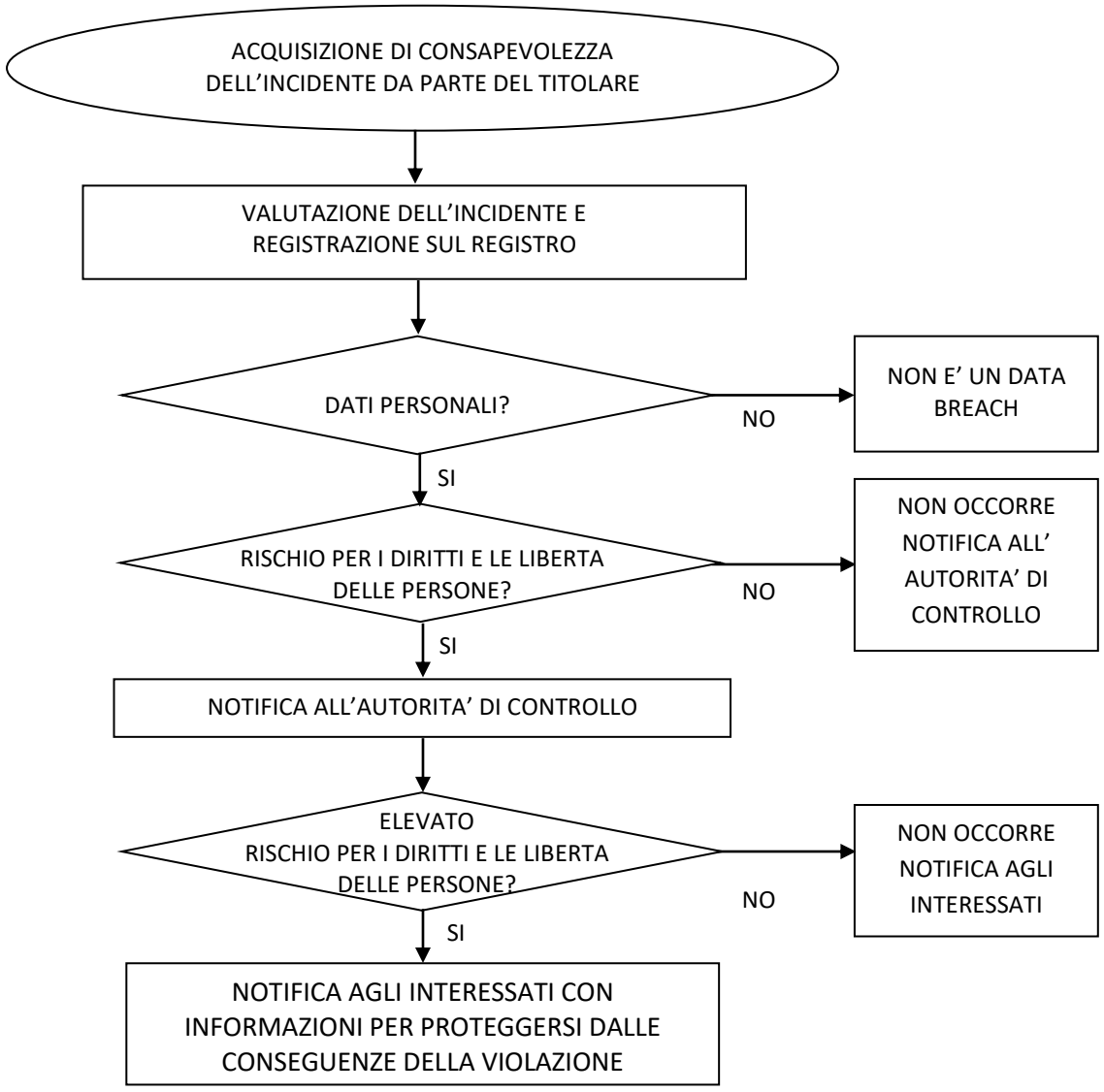
L'importanza di essere in grado di identificare una violazione, di valutare il rischio per gli individui e quindi di notificare se necessario, è sottolineata nel considerando 87 del RGPD: *"È opportuno verificare se siano state*

messe in atto tutte le misure tecnologiche e organizzative adeguate di protezione per stabilire immediatamente se c'è stata violazione dei dati personali e informare tempestivamente l'Autorità di Controllo e l'interessato. È opportuno stabilire il fatto che la notifica sia stata trasmessa senza ingiustificato ritardo, tenendo conto in particolare della natura e della gravità della violazione dei dati personali e delle sue conseguenze e effetti negativi per l'interessato. Siffatta notifica può dar luogo a un intervento dell'Autorità di Controllo nell'ambito dei suoi compiti e poteri previsti dal presente regolamento".

In caso di mancata notifica all'Autorità di Controllo o agli interessati quando richiesto dalla norma, così come l'assenza o l'inadeguatezza di misure di sicurezza potrebbero comportare, da parte dell'autorità di vigilanza, l'applicazione di sanzioni amministrative a un livello che sia efficace, proporzionato e dissuasivo entro il limite dell'inadempimento più grave (fino ad un totale di 20.000.000 € o al 4% del fatturato globale).

6. PIANO DI GESTIONE DEGLI INCIDENTI DI SICUREZZA

Al verificarsi di un incidente di sicurezza, si attiva un processo di gestione come di seguito illustrato:



7. LA CONSAPEVOLEZZA DELL'INCIDENTE

L'Art. 33 del RGPD richiede che, in caso di violazione dei dati personali, il titolare del trattamento la notifichi all'Autorità di Controllo entro 72 ore dal momento in cui ne è venuto a conoscenza. Il WP29 ritiene che un titolare debba essere considerato "*consapevole*" quando quel titolare ha un ragionevole grado di certezza che si è verificato un incidente di sicurezza che ha portato a compromettere i dati personali.

Tale grado di consapevolezza non è sempre evidente e nasce dall'essere venuti a conoscenza di un evento che potrebbe compromettere la riservatezza, la disponibilità o l'integrità delle informazioni. Da tale rilevazione deve scaturire il successivo step di valutazione dell'incidente, al fine di determinare se si tratti o meno di una violazione di dati personali.

La rilevazione dell'incidente viene effettuata da uno dei Referenti del Titolare; ogni Referente agisce su propria iniziativa per gli incidenti verificatisi nella sua area e ai suoi collaboratori o su espresso impulso del Segretario Generale. Chiunque rimarchi un incidente, deve darne comunicazione a mezzo email senza indugio al Referente competente per il contesto in cui si è rilevato l'incidente, utilizzando il modello allegato (allegato 3) e partecipando alla fase di valutazione dell'incidente, fornendo ogni ulteriore elemento utile.

In caso di rilevazione di una violazione da parte di un Responsabile del Trattamento, questo è tenuto a comunicare al Titolare con la massima urgenza, ed in ogni caso entro 24 ore dalla rilevazione della violazione, tutte le informazioni disponibili relative all'accaduto. Il Responsabile è tenuto a prestare ogni più ampia assistenza al Titolare al fine di consentirgli di assolvere agli obblighi di cui agli artt. 32-34 del RGPD.

8. LA VALUTAZIONE DELL'INCIDENTE

La consapevolezza che un incidente di sicurezza rappresenti una violazione di dati personali è funzione della rilevazione dell'incidente, della presa d'atto che siano coinvolti dati personali e della valutazione che tale evento possa comportare un rischio per i diritti e le libertà delle persone.

Pertanto, al momento della rilevazione dell'incidente, il titolare, tramite il proprio referente designato, deve immediatamente attivarsi per valutare se esso possa comportare un rischio di tale entità, in funzione di diversi aspetti fra cui:

- La numerosità dei soggetti che potrebbero essere danneggiati da tale evento;
- Le categorie dei soggetti a cui i dati si riferiscono, con particolare attenzione per categorie come minori, soggetti con disabilità o particolari forme di vulnerabilità;
- La tipologia dei dati coinvolti, con specifica cautela per le categorie di dati particolari di cui all'Art. 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10 del RGPD;
- La confidenza del fatto che le misure tecnologiche e organizzative implementate possano o meno aver impedito la compromissione dei dati oggetto dell'incidente di sicurezza.

Oltre all'analisi dell'incidente per verificare se sono coinvolti dati personali, è necessario attuare le conseguenti azioni per rimediare alle conseguenze dell'incidente ed eventualmente procedere con le notifiche necessarie.

Si riportano nell'allegato 1 alcuni casi, a titolo esemplificativo ma non esaustivo, che possano chiarire meglio quali tipologie di incidenti si traducano in violazioni di sicurezza che debbano comportare la notifica all'Autorità di Controllo ed eventualmente agli stessi interessati.

Anche qualora l'incidente non si traducesse in una violazione di sicurezza, tale evento deve essere registrato sull'apposito registro al fine di poter produrre evidenza documentale delle azioni intraprese in caso di verifica da parte dell'Autorità di Controllo. Sul registro devono essere rilevati gli estremi dell'incidente, le conseguenze che ha portato, le azioni intraprese per ridurne o annullarne l'impatto e la loro efficacia. All'allegato 2 è riportato il modello per la registrazione degli incidenti.

Nelle fasi di valutazione dell'incidente, qualora lo ritenga necessario il referente del titolare può avvalersi del supporto del Responsabile per la Protezione dei Dati al fine di determinare l'eventualità di procedere con le notifiche della violazione di sicurezza, in caso di bisogno.

9. LA NOTIFICA ALL'AUTORITA' DI CONTROLLO

L'Art. 33 del RGPD richiede che il titolare del trattamento notifichi all'Autorità di Controllo la violazione di dati personali entro 72 ore dal momento in cui ne è venuto a conoscenza. La comunicazione deve almeno

a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
c) identificare le probabili conseguenze della violazione dei dati personali;
d) illustrare le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Nel caso non siano disponibili informazioni precise e complete, è comunque necessario effettuare prontamente la comunicazione, focalizzandosi sugli effetti avversi della violazione piuttosto che sulla precisione della segnalazione. Sarà poi possibile fornire successivamente ulteriori informazioni ad integrazione di quanto già segnalato, come recita l'Art. 34 del RGPD: *"Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo"*.

Il soggetto designato dal titolare per effettuare materialmente la comunicazione è il referente, il quale procede ad istruire la documentazione necessaria che verrà comunicata all'Autorità Garante della Privacy. Il modello utilizzato per la comunicazione è reso disponibile sul sito dell'Autorità di Controllo, nella sezione specifica dedicata al Data Breach. La notifica deve essere inviata al Garante tramite posta elettronica all'indirizzo protocollo@pec.gpdp.it e deve essere sottoscritta digitalmente (con firma elettronica qualificata/firma digitale) ovvero con firma autografa. In quest'ultimo caso la notifica deve essere presentata unitamente alla copia del documento d'identità del firmatario.

L'oggetto del messaggio deve contenere obbligatoriamente la dicitura “NOTIFICA VIOLAZIONE DATI PERSONALI” e opzionalmente la denominazione del titolare del trattamento. Per maggiori informazioni occorre fare riferimento al sito ufficiale dell’Autorità di Controllo: http://www.garanteprivacy.it/.

10. LA NOTIFICA AGLI INTERESSATI

L’Art. 34 del RGPD stabilisce che *“Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all’interessato senza ingiustificato ritardo”*.

Il rischio elevato non è facilmente classificabile, tuttavia esiste senza dubbio quando la violazione può comportare un danno fisico, materiale o immateriale per le persone i cui dati sono stati violati. Esempi di tale danno sono la discriminazione, il furto d'identità o la frode, la perdita finanziaria e il danno alla reputazione. Quando la violazione riguarda dati personali che rivelano origini razziali o etniche, opinioni politiche, religione o convinzioni filosofiche, o appartenenza sindacale, o dati genetici, dati relativi alla salute o dati relativi alla vita sessuale, condanne penali e reati o relative misure di sicurezza, è molto probabile che si verifichi un rischio elevato per i diritti e le libertà degli interessati.

La soglia di comunicazione delle violazioni agli interessati è più alta rispetto a quella della comunicazione all’Autorità di Controllo, al fine di non sovraccaricarli di comunicazioni eccessive. La principale finalità della comunicazione agli interessati è quella di fornire loro specifiche informazioni per potersi proteggere dalle conseguenze della violazione. Pertanto, deve descrivere con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contenere almeno le seguenti informazioni:

- una descrizione della natura della violazione;
- il nome e i dati di contatto del responsabile della protezione dei dati o di altri punti di contatto; una descrizione delle probabili conseguenze della violazione;
- una descrizione delle misure adottate o proposte per affrontare la violazione, comprese, se del caso, misure per mitigarne gli eventuali effetti negativi.

Ad esempio, si possono invitare gli interessati a resettare eventuali password qualora le loro credenziali di accesso ad un servizio siano state violate.

Come prima scelta è preferenziale ricorrere al contatto diretto e dedicato degli interessati (es. email, SMS e messaggi diretti), a meno che questo non comporti uno sforzo sproporzionato rispetto alla finalità. E’ fortemente raccomandato l’utilizzo di differenti canali di comunicazione in contemporanea, al fine di massimizzare la possibilità di contattare il maggior numero di interessati colpiti dalla violazione, anche con il supporto di media di grande diffusione qualora il rischio lo richieda.

L'Art. 34 del RGPD stabilisce tre condizioni che, se soddisfatte, non richiedono la notifica ai singoli in caso di violazione. Questi sono:

- Il titolare del trattamento ha applicato misure tecniche e organizzative adeguate per proteggere i dati personali prima della violazione, in particolare quelle misure che rendono i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi. Ciò potrebbe, ad esempio, includere la protezione dei dati personali con la crittografia allo stato dell'arte o mediante la tokenizzazione.

- Immediatamente dopo una violazione, il titolare del trattamento ha provveduto a garantire che l'alto rischio posto ai diritti e alle libertà delle persone non si concretizzasse più. Ad esempio, a seconda delle circostanze del caso, il titolare può aver immediatamente identificato e intrapreso un'azione contro l'individuo che ha avuto accesso ai dati personali prima di poter compiere qualsiasi azione con gli stessi. È necessario tenere in debito conto le possibili conseguenze di eventuali violazioni della riservatezza, anche in questo caso, a seconda della natura dei dati in questione.
- Comporterà uno sforzo sproporzionato per contattare le persone, quando forse i loro dettagli di contatto sono stati persi a causa della violazione o non sono noti in primo luogo. Ad esempio, il magazzino di un ufficio statistico si è allagato e i documenti contenenti dati personali sono stati memorizzati solo in formato cartaceo. In tali casi, il titolare deve fare una comunicazione pubblica o adottare una misura simile, in base alla quale le persone possano essere informate in modo altrettanto efficace. Nel caso di uno sforzo sproporzionato, potrebbero anche essere previste disposizioni tecniche per rendere le informazioni sulla violazione disponibili su richiesta, che potrebbero rivelarsi utili per i soggetti interessati da una violazione, che il titolare del trattamento non può contattare in maniera alternativa.

Conformemente col principio di *accountability* che è alla base del RGPD, il titolare del trattamento dovrebbe essere in grado di dimostrare all'Autorità di Controllo di soddisfare una o più delle condizioni sopra indicate. Va tenuto presente che, sebbene la notifica inizialmente non possa essere richiesta se non vi è alcun rischio per i diritti e le libertà delle persone fisiche, ciò potrebbe cambiare nel tempo e il rischio dovrebbe essere rivalutato.

11. ALLEGATI DEL PRESENTE DOCUMENTO

Si riportano di seguito gli allegati al presente documento, che ne costituiscono parte integrante:

Allegato B1 – Esempi di incidenti di sicurezza e valutazione di eventuali violazioni

Allegato B2 – Modello Registro delle Violazioni di dati personali

Allegato B3- Informazioni da comunicare al Referente

12. APPROVAZIONE E REVISIONE DEL PRESENTE DOCUMENTO

Il presente documento sarà approvato dall'Ente tramite Delibera di Giunta Comunale.

Il documento sarà soggetto a modifiche ed aggiornamenti ogni qualvolta si renderà necessario. Tali aggiornamenti saranno rilevati dal Responsabile per la Protezione dei Dati, che ne verificherà la rispondenza ai termini di legge.

Le modifiche al documento verranno approvate con Delibera di Giunta Comunale o Determinazione Dirigenziale da parte del responsabile del procedimento a cui fa capo il servizio Sistema Informatico (a seconda della rilevanza delle modifiche apportate).

ALLEGATO B1 – ESEMPI DI INCIDENTI DI SICUREZZA E VALUTAZIONE DI EVENTUALI VIOLAZIONI

I seguenti esempi sono tratti all'allegato B delle Guidelines on Personal Data breach notification under Regulation 2016/679 - fonte Article 29 Data Protection Working Party:

ESEMPIO	NOTIFICA AUTORITA' CONTROLLO	NOTIFICA ALL'INTERESSATO	NOTE / RACCOMANDAZIONI
Un titolare ha fatto un backup di un archivio di dati personali crittografati su una chiave USB. La chiave viene rubata.	NO	NO	Finché i dati vengono crittografati con un algoritmo avanzato, i backup dei dati esistono, la chiave univoca non viene compromessa e i dati possono essere ripristinati in tempo utile, ciò potrebbe non essere una violazione segnalabile. Tuttavia, se viene successivamente compromesso, è necessaria la notifica.
Un titolare gestisce un servizio online. A seguito di un attacco informatico su quel servizio, i dati personali degli individui vengono rubati. Il titolare ha clienti in un singolo stato membro,	Sì, riferire all'autorità di vigilanza se vi sono probabili conseguenze per le persone.	Sì, riferire alle persone a seconda della natura dei dati personali interessati e se la gravità delle probabili conseguenze per gli individui è elevata.	
Una breve interruzione di corrente di alcuni minuti presso il call center di un titolare	NO	NO	Questa non è una violazione soggetta a notifica, ma è comunque un incidente registrabile ai sensi dell'articolo 33, paragrafo 5.

comporta che i clienti non siano in grado di chiamare il titolare e accedere ai loro record.			I registri appropriati devono essere conservati dal titolare.
Un titolare subisce un attacco ransomware che provoca la crittografia di tutti i dati. Non sono disponibili backup 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 c'erano altri malware presenti nel sistema.	Sì, riferire all'autorità di vigilanza, se ci sono probabili conseguenze per gli individui in quanto si tratta di una perdita di disponibilità.	Sì, riferire ai singoli, 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 ai singoli in quanto non vi sarebbe stata alcuna perdita permanente di disponibilità o riservatezza. Tuttavia, se l'autorità di vigilanza venisse a conoscenza dell'incidente con altri mezzi, potrebbe prendere in considerazione un'indagine per valutare la conformità ai requisiti di sicurezza più ampi dell'articolo 32.
Un individuo telefona al call center di una banca per segnalare una violazione dei dati. L'individuo ha ricevuto una dichiarazione mensile di qualcun altro. Il titolare del trattamento intraprende un'investigazione breve (ossia completata entro 24 ore) e stabilisce con ragionevole certezza che si è verificata una violazione dei dati personali e che vi è un difetto sistemico che potrebbe significare che altri individui sono o potrebbero essere interessati.	SI	Solo le persone colpite vengono avvisate se c'è un rischio elevato ed è ragionevolmente certo che altri soggetti non siano 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 titolare effettua il passaggio aggiuntivo per notificare agli altri individui se vi è un rischio elevato per loro.
Un titolare gestisce un sito di e-commerce ed ha clienti in più Stati membri. Il sito subisce	Sì, segnalare all'autorità di vigilanza principale se il	Sì, in quanto potrebbe comportare alto rischio.	Il titolare dovrebbe agire, ad es. forzando il ripristino della password degli account interessati,

un attacco informatico e usernames, password e cronologia degli acquisti sono pubblicati online dall'attaccante.	trattamento è transfrontaliero.		nonché altri passaggi per mitigare il rischio. Il titolare del trattamento dovrebbe anche considerare qualsiasi altro obbligo di notifica, ad es. sotto la direttiva NIS come fornitore di servizi digitali.
Una società di hosting di siti Web che agisce come responsabile del trattamento identifica un errore nel codice che controlla l'autorizzazione degli utenti. L'effetto del difetto indica che ogni utente possa accedere ai dettagli dell'account di qualsiasi altro utente.	In qualità di responsabile, la società di hosting del sito web deve notificare i clienti interessati (i titolari) senza indebito ritardo. Supponendo che la società di hosting del sito web abbia condotto le proprie indagini, i titolari coinvolti dovrebbero essere ragionevolmente certi se vi sia stata una violazione, pertanto è probabile che venga considerato come "presa di coscienza" una volta che sia stata notificata dalla società di hosting (il responsabile). Il titolare deve quindi informare l'autorità di vigilanza.	Se non ci sono probabili rischi elevati per le persone la violazione non deve essere notificata.	La società di hosting del sito web (responsabile) deve considerare qualsiasi altro obbligo di notifica (ad esempio ai sensi della direttiva NIS come fornitore di servizi digitali). Se non vi è alcuna prova che tale vulnerabilità sia sfruttata per uno dei suoi titolari, una violazione notificabile potrebbe non essersi verificata, ma potrebbe essere verosimilmente registrabile o essere oggetto di non conformità ai sensi dell'articolo 32.
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 la violazione come ad alto rischio per il	Sì, occorre riferire alle persone colpite.	

	benessere del paziente e per la sua privacy.		
I dati personali di un gran numero di studenti vengono erroneamente inviati alla mailing list sbagliata con più di 1000 destinatari.	Sì, occorre riferire all'Autorità di Vigilanza.	Sì, occorre riferire alle persone in base alla portata e al tipo di dati personali coinvolti, oltre che alla gravità delle possibili conseguenze.	
Una email di marketing diretto viene inviata ai destinatari nei campi "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 le password iniziali).	Sì, occorre riferire alle persone 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.

ALLEGATO B2 – MODELLO REGISTRO VIOLAZIONI DEI DATI PERSONALI

Registro Violazioni dati personali (Data Breach)

Registro		Dettagli della Violazione					Conseguenze della Violazione	Misure Intraprese / Da intraprendere			
N.	Ticket Rif.	Data Evento	Natura dell'Evento	Descrizione della Violazione	Dati Interessati	Soggetti Coinvolti		Informativa Garante	Informativa altri soggetti coinvolti	Azioni Intraprese	Azioni da Intraprendere
1											
2											
3											
4											
5											
6											
7											
8											
9											
10											
11											
12											
13											
14											
15											
16											
17											
18											
19											
20											

ALLEGATO B3 - INFORMAZIONI DA COMUNICARE AL REFERENTE

Dati identificativi Segnalante	
Eventuali Contatti (altre informazioni)	

INFORMAZIONI DI SINTESI DELLA VIOLAZIONE

Quando si è verificata la violazione dei dati personali trattati nell'ambito della banca dati?

- ☐ Il _____
- ☐ Dal _____(la violazione è ancora in corso)
- ☐ Dal _____ al _____
- ☐ In un tempo non ancora determinato

Ulteriori informazioni circa le date in cui è avvenuta la violazione:

_____
_____

Data: _____ Ora: _____ in cui si è venuto a conoscenza della violazione

In caso di segnalazione oltre le 72 ore, quali sono i motivi del ritardo?

_____
_____

Breve descrizione della violazione:

_____
_____
_____
_____
_____
_____

Tipo di violazione

- ☐ Lettura (presumibilmente i dati non sono stati copiati)
- ☐ Copia (i dati sono ancora presenti sui sistemi del titolare)
- ☐ Alterazione (i dati sono presenti sui sistemi ma sono stati alterati)
- ☐ Cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione)
- ☐ Furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione)
- ☐ Altro : _____

Causa della violazione

- ☐ Azione intenzionale interna
- ☐ Azione accidentale interna
- ☐ Azione intenzionale esterna
- ☐ Azione accidentale esterna
- ☐ Sconosciuta
- ☐ Altro (specificare)

Categorie di dati personali oggetto di violazione

- ☐ 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
- ☐ Categorie ancora non determinate
- ☐ Altro _____

Indicare il volume (anche approssimativo) dei dati personali oggetto di violazione

- ☐ N. _____
- ☐ Circa n. _____
- ☐ Un numero (ancora) sconosciuto di dati

Indicare le tipologie di interessati coinvolti nella violazione (dipendenti, utenti, cittadini, minori, persone vulnerabili, altro:

_____
_____
_____
_____
_____

Numero (anche approssimativo) di interessati coinvolti nella violazione

- ☐ N. _____ interessati
- ☐ Circa n. _____ interessati
- ☐ Un numero (ancora) sconosciuto di interessati

Che tipo di dati sono oggetto di violazione?

- □ Dati anagrafici/codice fiscale
- □ Dati di accesso e di identificazione (user name, password, customer ID, altro)
- □ Dati relativi a minori
- □ Dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale
- □ Dati personali idonei a rivelare lo stato di salute e la vita sessuale
- □ Dati giudiziari
- □ Copia per immagine su supporto informatico di documenti analogici
- □ Ancora sconosciuto
- □ Altro : _____

Livello di gravità della violazione dei dati personali trattati nell'ambito della banca dati (secondo le valutazioni del titolare)?

- □ Basso/trascurabile
- □ Medio
- □ Alto
- □ Molto alto

Misure tecniche e organizzative adottate (o di cui si propone l'adozione20) per porre rimedio alla violazione e ridurne gli effetti negativi per gli interessati

_____
_____
_____
_____
_____

Misure tecniche e organizzative adottate (o di cui si propone l'adozione) per prevenire simili violazioni future

_____
_____
_____
_____
_____

La violazione è stata comunicata anche agli interessati?

- □ Sì, in data _____ tramite □ SMS / □ Posta cartacea / □ Posta Elettronica / □ Altro
- □ No, perché _____

Qual è il contenuto della comunicazione resa agli interessati?

_____
_____
_____
_____