PROCEDURA OPERATIVA

Gestione della violazione dei dati
(Data Breach)

Rev. 2 del 21/11/2019

Stato delle revisioni

Rev	*Data*	*Motivo della modifica*	*Redatta da*	*Approvata da*
1	21/05/2018	Prima emissione	RPD/DPO	Titolare
2	21/11/2018	Aggiornamento tecnico	RPD/DPO	Titolare

Allegati

Codice	*Descrizione*
MOPD 07-001	Scheda segnalazione incidente
MOPD 07-002	Rilevazione e valutazione violazione dati
MOPD 07-003	Registro violazioni dati personali

1. SCOPO

Scopo della presente procedura è di fornire istruzioni precise e dettagliate nel caso succeda un incidente di sicurezza, e nello specifico una violazione dei dati personali. Assicurare il sistematico trattamento di qualunque violazione dei dati personali, ai sensi degli artt. 33 e 34 del Regolamento europeo UE 2016/679.

2. CAMPO DI APPLICAZIONE

Questa procedura si applica a tutti gli incidenti di sicurezza delle informazioni rilevati, indipendentemente dal processo in cui esse sono state evidenziate e da quello che è stato identificato causa del problema.

3. RIFERIMENTI NORMATIVI E DOCUMENTALI

Parlamento Europeo	RGPD/GDPR 679/2016 - Regolamento europeo nr. 679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (abroga la direttiva 95/46/CE)
Gruppo di lavoro art. 29 WP29	Linee guida sul data breach (violazione dei dati)

4. TERMINI E DEFINIZIONI

Violazione dei dati personali	(art. 4, paragrafo 12 del GDPR) 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
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
Banca di dati	Qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti

5. MODALITA' OPERATIVE

Per violazione dei dati personali (in seguito "data breach") si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati dall'Organizzazione.

Il personale addetto al trattamento, qualora venga a conoscenza nell'espletamento delle attività di competenza o indirettamente nello svolgimento delle stesse, del verificarsi di eventuali violazioni dei dati personali o di incidenti informatici che possano esporre a rischio di violazione dei dati (data breach), deve tempestivamente informare il Titolare, attraverso il Responsabile Protezione Dati.

Il Titolare, ove ritenga probabile che dalla violazione dei dati *possano derivare rischi per i diritti e le libertà degli interessati*, provvede alla notifica della violazione all'Autorità di controllo (Garante per la Protezione dei Dati Personali). La notifica dovrà avvenire entro 72 ore e comunque senza ingiustificato ritardo.

Il Responsabile del trattamento è obbligato ad informare il Titolare, senza ingiustificato ritardo, dopo essere venuto a conoscenza della violazione.

I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, in conformità al considerando 75 del RGPD, sono i seguenti:

- danni fisici, materiali o immateriali alle persone fisiche;
- perdita del controllo dei dati personali;
- limitazione dei diritti, discriminazione;
- furto o usurpazione d'identità;
- perdite finanziarie, danno economico o sociale.
- decifratura non autorizzata della pseudonimizzazione;
- pregiudizio alla reputazione;
- perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari).

Se il Titolare ritiene che il rischio per i diritti e le libertà degli interessati conseguente alla violazione rilevata **è elevato**, allora deve informare questi ultimi, senza ingiustificato ritardo, con un linguaggio semplice e chiaro al fine di fare comprendere loro la natura della violazione dei dati personali verificatesi. I rischi per i diritti e le libertà degli interessati possono essere considerati "elevati" quando la violazione può, a titolo di esempio:

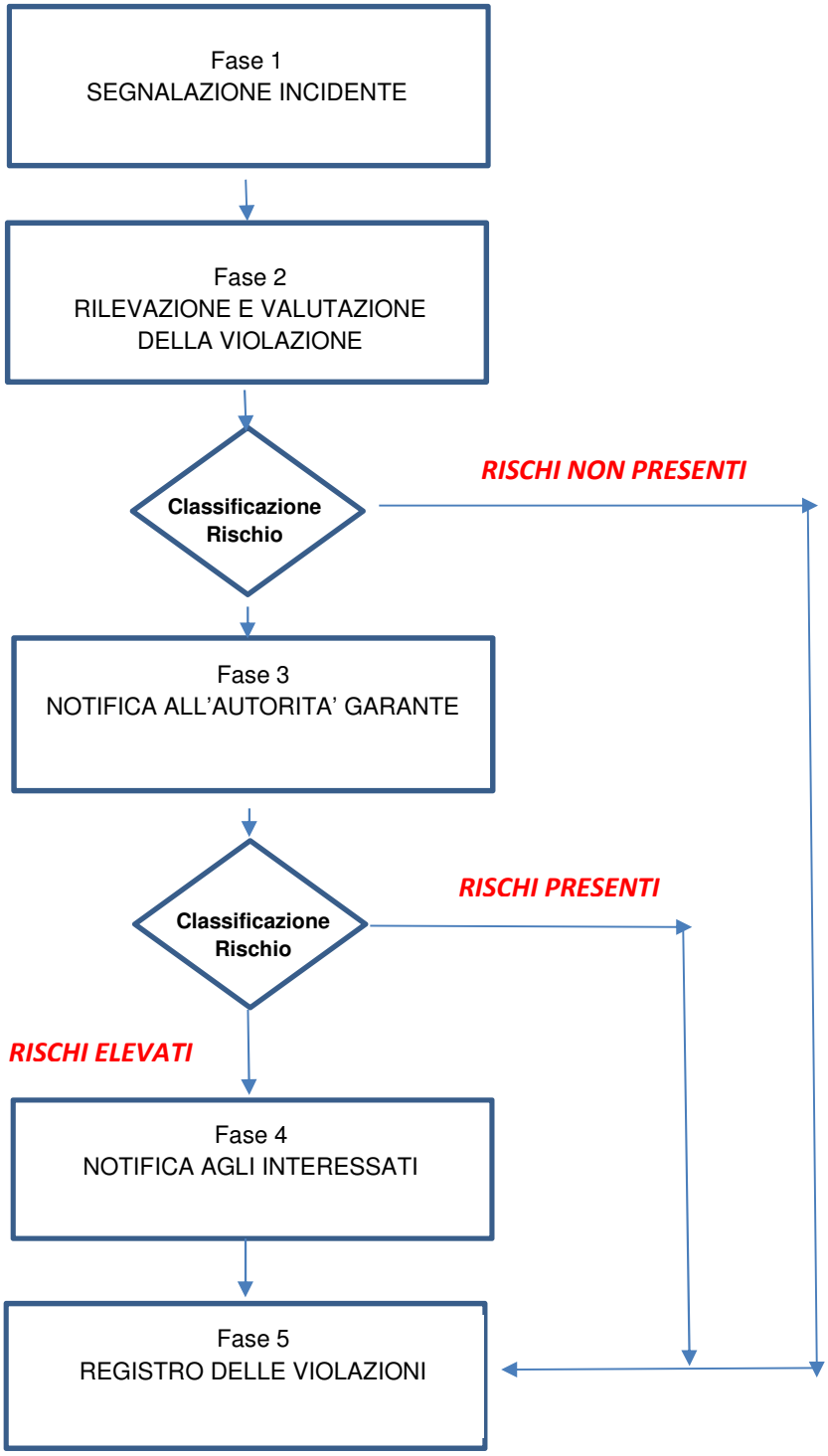
- coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;
- riguardare categorie particolari di dati personali;
- comprendere dati che possono accrescere ulteriormente i potenziali rischi (ad esempio dati di localizzazione, finanziari, relativi alle abitudini e preferenze);
- comportare rischi imminenti e con un'elevata probabilità di accadimento (ad esempio rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito);
- impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (ad esempio utenti deboli, minori, soggetti indagati).

La notifica deve avere il contenuto minimo previsto dall'art. 33 RGPD, ed anche la comunicazione all'interessato deve contenere almeno le informazioni e le misure di cui al citato art. 33.

Il Titolare deve opportunamente documentare le violazioni di dati personali subite, anche se non comunicate alle autorità di controllo, nonché le circostanze ad esse relative, le conseguenze e i provvedimenti adottati o che intende adottare per porvi rimedio. Tale documentazione deve essere conservata con la massima cura e diligenza in quanto può essere richiesta dall'Autorità di Controllo al fine di verificare il rispetto delle disposizioni del RGPD.

Flusso di gestione della violazione

Il presente paragrafo descrive il processo e il relativo flusso di attività che il Titolare del trattamento dovrebbe seguire in caso di rilevazione di una violazione ai dati.



Fase 1 – SEGNALAZIONE INCIDENTE

1.1.	Addetti trattamento Responsabile Protezione Dati (RPD)	Il personale addetto al trattamento, qualora venga a conoscenza nell'espletamento delle attività di competenza o indirettamente nello svolgimento delle stesse, del verificarsi di eventuali violazioni dei dati personali o di incidenti informatici che possano esporre a rischio di violazione dei dati (data breach), deve tempestivamente informare il Titolare, attraverso il Referente Privacy Interno.	*Modulo MOPD 07-001*

Fase 2 – RILEVAZIONE E VALUTAZIONE DELLA VIOLAZIONE

2.1	Responsabile Responsabile Protezione Dati (RPD)	• Identificare tempestivamente l'avvenuta violazione; • Stabilire la tipologia di violazione, le cause e i danni eventualmente provocati ai sistemi e ai dati; • Comunicare quanto occorso al Titolare e al Responsabile Protezione Dati (DPO), se presente, e al Referente Privacy Interno; • Coinvolgere le aree di business impattate dalla violazione	*Modulo MOPD 07-002*
2.2	Titolare DPO Responsabile Esperto IT	Effettua una analisi della violazione tenendo in considerazione: • la quantità dei dati personali • la tipologia dei dati violati • la quantità di soggetti interessati coinvolti • la tipologia dei soggetti interessati coinvolti • le aree di business coinvolte e l'impatto sul business	*Modulo MOPD 07-002*
2.3	Titolare Responsabile Esperto IT Responsabile Protezione Dati (RPD)	Identificare i rischi conseguenti l'evento per i diritti e le libertà degli interessati, tenendo in considerazione le misure preventive attuate per far fronte ai danni (crittografia e pseudonimizzazione dei dati) Classificare i rischi della violazione in: • **NON PRESENTI** quando la violazione non ha alcuna conseguenza dimostrabile sui diritti e le libertà degli interessati • **PRESENTI** quando la violazione ha effetti negativi sui diritti e le libertà degli interessati ma non sono elevati per la natura della violazione, per la quantità si soggetti o dati coinvolti, oppure sono state adottate misure preventive per limitarli come la crittografia o la pseudonimizzazione ; • **ELEVATI** quando la violazione comporta rischi rilevanti per i diritti e le libertà degli interessati, coinvolge un elevato numero di interessati e dati e non sono state adottate misure preventive di protezione	*Modulo MOPD 07-002*

Fase 3 – NOTIFICA ALL'AUTORITA' GARANTE

3.1	Titolare Responsabile Responsabile Protezione Dati (RPD)	Tempestivamente, si consiglia entro e non oltre le 48 ore dal Punto 2.1, di raccogliere e rielaborare le seguenti informazioni in merito alla violazione: • natura e breve descrizione della violazione dei dati; • data e ora in cui la violazione si è verificata; • data e ora in cui la violazione è stata rilevata; • luogo in cui si è verificata la violazione • dispositivi oggetto della violazione • breve descrizione dei sistemi di elaborazione o memorizzazione dei dati coinvolti nella violazione e relativa ubicazione; • categorie e numero approssimativo di soggetti interessati coinvolti; • tipologia e numero approssimativo di dati personali oggetto della violazione; • probabili conseguenze della violazione sui dati personali;	*Modulo MOPD 07-002*

		• livello di rischio conseguente la violazione; • misure tecniche e organizzative adottate o che il Titolare intende adottare per limitare la violazione e gli effetti negativi; • se la violazione è stata o sarà comunicata ai soggetti interessati o, in caso contrario, le motivazioni per cui non sarà comunicata la violazione ai soggetti interessati; • contenuto della comunicazione agli interessati e il canale utilizzato per la comunicazione; • se la violazione coinvolge altri soggetti terzi; • se la violazione coinvolge altri Paesi dell'Unione Europea; • nome e dati di contatto del Data Protection Officer o di altro punto di contatto per l'Autorità.	
3.2	Titolare Responsabile Responsabile Protezione Dati (RPD)	Tempestivamente, ***entro e non oltre 72 ore*** dal punto 2.1: • accedere alla sezione del sito dell'Autorità Garante per la protezione dei dati personali dedicata alla notifica in caso di violazioni; • compilare il modulo di notifica telematico con le informazioni già raccolte in precedenza, sopra descritte; • inviare la notifica	*Modulo MOPD 07-002* *Modello di notifica telematico*
3.3	Titolare Responsabile Responsabile Protezione Dati (RPD)	Se per motivi organizzativi e tecnici, la notifica all'Autorità Garante non è stata effettuata entro e non oltre le 72 ore dal punto 2.1: • integrare il modulo di notifica con la motivazione per cui la comunicazione è sopraggiunta in ritardo	
3.4	Titolare Responsabile Responsabile Protezione Dati (RPD)	Monitorare eventuali disposizioni o richieste di informazioni pervenute dall'Autorità Garante	

Fase 4 – NOTIFICA AGLI INTERESSATI

4.1	Titolare Responsabile
	
	Responsabile Protezione Dati (RPD)
		Immediatamente dopo l'avvenuta notifica al Garante, qualora i rischi individuati dal Titolare o dall'Autorità stessa siano "Elevati":
		• Coinvolgere il Titolare, le aree di business impattate dalla violazione;
		• stabilire se la notifica agli interessati possa in qualche modo compromettere eventuali indagini in corso relative alla violazione e, in tal caso, attendere per la notifica agli interessati;
		• rispettare eventuali indicazioni che l'Autorità Garante potrebbe fornire in tali circostanze;
		• individuare il mezzo più opportuno per la notifica agli interessati (posta elettronica, fax, sito internet, comunicati stampa, media, etc) tenendo in considerazione:
		  ○ la quantità di soggetti interessati coinvolti da raggiungere;
		  ○ il contesto aziendale;
		  ○ i mezzi normalmente utilizzati per comunicare con gli interessati;
		  ○ i costi.	

4.2	Titolare Responsabile	Predisporre la comunicazione agli interessati con un linguaggio semplice e chiaro indicando: • natura della violazione dei dati • probabili conseguenze della violazione	

	Responsabile Protezione Dati (RPD)	• misure tecniche e organizzative adottate e/o da adottare per limitare la violazione; • eventuali raccomandazioni per imitare gli eventuali danni;	
4.3	Titolare Responsabile Responsabile Protezione Dati (RPD)	Inviare la comunicazione e monitorare i riscontri da parte degli interessati.	

Fase 5 – REGISTRO DELLE VIOLAZIONI

5.1	Responsabile Referente Privacy Interno	A conclusione di tutte le fasi precedenti, documentare la violazione dei dati personali all'interno di un apposito registro, in cui riportare: • le circostanze della violazione • le date di riferimento • le conseguenze della violazione • le misure adottate per porvi rimedio • copia della notifica all'Autorità Garante • se avvenuta, attestazione della notifica ai soggetti interessati (comunicazione di esempio, email, comunicato stampa, etc)	*Modulo MOPD 07-003*
5.2	Responsabile Responsabile Protezione Dati (RPD)	• Conservare il Registro delle violazioni e metterlo a disposizione dell'Autorità Garante o di chi la rappresenta, in caso di accertamenti	*Modulo MOPD 07-003*

6. RICHIAMO AL REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI
Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016

Articolo 33
Notifica di una violazione dei dati personali all'autorità di controllo
(C85, C87, C88)

1. In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.
2. Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.
3. La notifica di cui al paragrafo 1 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) descrivere le probabili conseguenze della violazione dei dati personali;
   d) descrivere 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.
4. 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.
5. Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo.

Articolo 34
Comunicazione di una violazione dei dati personali all'interessato (C86-C88)

1. 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.
2. La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d).
3. Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni:
    a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
    b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;
    c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.
4. Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta.

Considerandi

(85) Una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata. Pertanto, non appena viene a conoscenza di un'avvenuta violazione dei dati personali, il titolare del trattamento dovrebbe notificare la violazione dei dati personali all'autorità di controllo competente, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che il titolare del trattamento non sia in grado di dimostrare che, conformemente al principio di responsabilizzazione, è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Oltre il termine di 72 ore, tale notifica dovrebbe essere corredata delle ragioni del ritardo e le informazioni potrebbero essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

(86) Il titolare del trattamento dovrebbe comunicare all'interessato la violazione dei dati personali senza indebito ritardo, qualora questa violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà della persona fisica, al fine di consentirgli di prendere le precauzioni necessarie. La comunicazione dovrebbe descrivere la natura della violazione dei dati personali e formulare raccomandazioni per la persona fisica interessata intese ad attenuare i potenziali effetti negativi. Tali comunicazioni agli interessati dovrebbero essere effettuate non appena ragionevolmente possibile e in stretta collaborazione con l'autorità di controllo e nel rispetto degli orientamenti impartiti da questa o da altre autorità competenti quali le autorità incaricate dell'applicazione della legge. Ad esempio, la necessità di attenuare un rischio immediato di danno richiederebbe che la comunicazione agli interessati fosse tempestiva, ma la necessità di attuare opportune misure per contrastare violazioni di dati personali ripetute o analoghe potrebbe giustificare tempi più lunghi per la comunicazione.

(87) 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.

(88) Nel definire modalità dettagliate relative al formato e alle procedure applicabili alla notifica delle violazioni di dati personali, è opportuno tenere debitamente conto delle circostanze di tale violazione, ad esempio stabilire se i dati personali fossero o meno protetti con misure tecniche adeguate di protezione atte a limitare efficacemente il rischio di furto d'identità o altre forme di abuso. Inoltre, è opportuno che tali modalità e procedure tengano conto dei legittimi interessi delle autorità incaricate dell'applicazione della legge, qualora una divulgazione prematura possa ostacolare inutilmente l'indagine sulle circostanze di una violazione di dati personali.

Segnalazione da	**N°**	**Data**		
	❑ **Incidente**	❑ **Terzi**	❑ **Audit interno**	❑ **Altro**

Attività / Area	
Descrizione	
Segnalato da	
Valutazione cause	
Descrizione	
Trattamento	
Evidenze oggettive allegate	

Modello compilato da	
Segnalato a Titolare/ DPO / Responsabile	***Data***

Titolare del trattamento

Comune di ……..				
Indirizzo	*Prov:*		*Comune*	
	Cap		*Indirizzo*	
Persona addetta alla comunicazione				
Funzione rivestita				
Indirizzo PEC o email per eventuali comunicazioni				
Recapito telefonico				

Denominazione della/e banca/banche dati oggetto di data breach e breve descrizione della violazione dei dati personali ivi trattati

Quando si è verificata la violazione dei dati?

[ ] Il giorno _____
[ ] Tra il _____ e il _____
[ ] In un tempo non ancora determinato
[ ] E' possibile che sia ancora in corso

Dove è avvenuta la violazione dei dati? (specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)

Modalità di esposizione al rischio?

a) 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:

b) Dispositivo oggetto della violazione

[ ] Postazione di lavoro / computer
[ ] Rete
[ ] Dispositivo mobile
[ ] File o parte di un file
[ ] Strumento di backup
[ ] Documento cartaceo
[ ] Altro:

Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione

Quante persone sono state colpite dalla violazione di dati?

[ ] Nr. _____ di persone
[ ] Circa _____ persone
[ ] Un numero (ancora) sconosciuto di persone

Altri dati coinvolti nella 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 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 ed organizzative applicate ai dati colpiti dalla violazione

Quali misure tecnologiche e organizzative sono state assunte per contenere la violazione dei dati e prevenire simili violazioni future?

Valutazione dei rischi conseguenti l'evento per i diritti e le libertà degli interessati, tenendo in considerazione le misure preventive attuate per far fronte ai danni

[ ] NON PRESENTI [ ] PRESENTI [ ] ELEVATI

Natura della comunicazione

[ ] Nuova comunicazione
[ ] Inserimento ulteriori informazioni sulla precedente comunicazione (numero di riferimento) _____

La violazione è stata comunicata anche agli interessati?

[ ] Sì, è stata comunicata il _____
[ ] No, perché _____

La violazione coinvolge interessati che si trovano in altri Paesi UE?

[ ] Sì [ ] No

La comunicazione è stata effettuata alle competenti autorità di controllo?

[ ] No, perché _____
[ ] Sì

Anno di riferimento: _____

Data evento	Descrizione evento	Rimedi	Notifica interessati?	Notifica Autorità?	Note