Sistema di Gestione della Procedura di Data Breach (SGPDB)

GESTIONE PROCEDURA DATA BREACH

Mission della Procedura:
Definire le responsabilità e le modalità per il corretto adempimento all'obbligo di notifica al Garante privacy ed eventuale comunicazione agli interessati di violazioni di dati personali di cui agli artt. 33 e 34 GDPR

Conservatorio di Musica "Giuseppe Verdi"

Via Conservatorio, 12 – 20122 Milano

REVISIONE	DATA	MOTIVO DELLA REVISIONE
00	07/05/2018	Prima emissione della procedura ai sensi del Regolamento UE 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati

ATTIVITA'	DATA	FIRMA
Redazione della procedura (titolare, DPO, responsabile interno privacy)		
Verifica ed approvazione (Titolare e DPO)		

SOMMARIO

SCOPO E CAMPO DI APPLICAZIONE

Scopo della presente procedura è quello di definire le modalità e le responsabilità per il corretto adempimento dell'obbligo di notifica al Garante privacy ed eventuale comunicazione agli interessati di violazioni di dati personali.

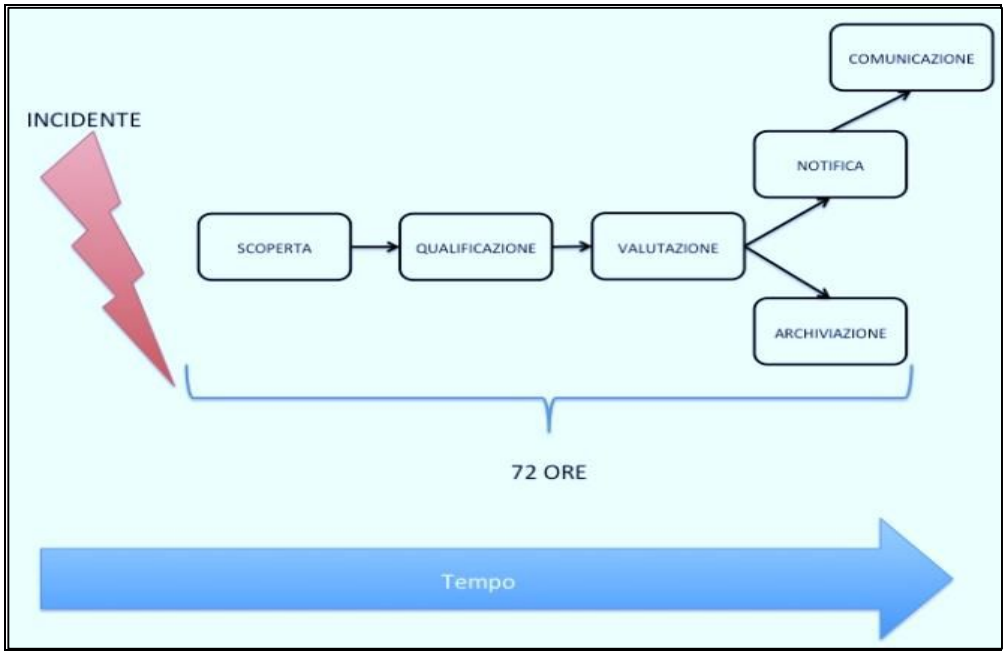
Le prescrizioni contenute nella presente procedura discendono da normative cogenti, decreti, linee guida, provvedimenti, considerati applicabili all'Organizzazione al fine di assicurare piena conformità del Sistema di gestione privacy alle stesse.

La presente procedura si applica in presenza di una violazione di dati personali ovvero qualora si verifichi (sia in maniera accidentale che illecita) la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

RIFERIMENTI NORMATIVI

NORME TECNICHE O COGENTI	RIFERIMENTI APPLICABILI
Regolamento (UE) 2016/679	Art.33 Notifica di una violazione dei dati personali all'Autorità di controllo Art. 34 Comunicazione di una violazione dei dai personali all'interessato
Linee guida Gruppo di lavoro articolo 29	Parte I - A e B Parte II - A, B, C Parte III – A, B, C, D
Provvedimenti Garante privacy	Provvedimento 4 aprile 2013, n.97 [doc. web n.2388260]
D.lgs. 196/2003	Art. 32-bis Adempimenti conseguenti ad una violazione di dati personali

MODALITA' OPERATIVE



<table>
<tr><th>FASI DI ATTUAZIONE</th><th>DESCRIZIONE DELLE FASI</th><th>MODULI CORRELATI</th><th>FUNZIONI AZIENDALI INTERESSATE</th></tr>
<tr>
<td>SCOPERTA DELLA VIOLAZIONE
  </td>
<td>Il RESPONSABILE del trattamento (o la persona che viene a conoscenza della violazione, es. fornitore in caso di trattamento affidato ad un responsabile esterno) notifica la violazione dei dati al titolare del trattamento e al DPO (ove nominato) senza ingiustificato ritardo (ovvero entro 8 ore).
Dal momento della notifica il Titolare si ritiene a “conoscenza” della violazione.
E’ “a conoscenza” il titolare che abbia un ragionevole grado di certezza in merito alla verificazione di un incidente di sicurezza.
Nel caso di violazioni di difficile rilevazione, sarà necessario instaurare un’indagine più approfondita.
In questi casi, durante la fase di “investigazione”, il titolare può essere considerato come privo di un grado di conoscenza tale da far scattare immediatamente l’obbligo di notifica.
Ad ogni modo, il diligente comportamento del titolare sarà in ogni caso valutato sulla base della sua tempestiva attivazione in caso venga informato di una possibile infrazione; la fase “investigativa” non deve dunque essere abusata per prorogare illegittimamente il termine di notifica.
E’ importante poter dimostrare il momento della scoperta della violazione, poiché da tale momento decorrono le 72 ore per la notifica al Garante ed eventuale comunicazione agli interessati.
Pertanto, la comunicazione al titolare e al DPO (ove nominato) va effettuata in forma scritta (es. via mail, Pec, etc.) riportando almeno gli elementi di cui alla sottostante tabella oltre ad eventuali altre informazioni aggiuntive:

<table>
<tr><td>Data scoperta violazione</td><td></td></tr>
<tr><td>Data comunicazione al Titolare (e al DPO)</td><td></td></tr>
<tr><td>Altri soggetti a cui è stata inviata comunicazione (es. IT)</td><td></td></tr>
<tr><td>Modalità ulteriori di comunicazione (mail, etc.)</td><td></td></tr>
<tr><td>Rilevazione da parte di</td><td></td></tr>
<tr><td>Descrizione della violazione</td><td></td></tr>
<tr><td>Analisi della causa violazione</td><td></td></tr>
<tr><td>Prima valutazione dell’impatto per gli interessati (non grave/grave/gravissimo) e motivazione</td><td></td></tr>
<tr><td>Correzione o azione correttiva proposta a tamponamento della violazione</td><td></td></tr>
</table>

Per “violazione di dati” 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 ai dati personali trasmessi, conservati o comunque trattati.

Esempi di violazione:
- Perdita accidentale: es. smarrimento di una chiavetta USB contenente dati riservati;
- Furto: ad es. furto di un notebook contenente dati confidenziali;
- Infedeltà aziendale: es. persona interna all’organizzazione che avendo autorizzazione ad accedere ai dati ne produce copia distribuita in ambiente pubblico;
- Accesso abusivo: es. accesso non autorizzato ai sistemi informatici con successiva divulgazione delle informazioni acquisite.</td>
<td>E-mail, Pec,</td>
<td><u>Responsabile</u>:

RESPONSABILE DEL TRATTAMENTO (o la persona che viene a conoscenza della violazione)</td>
</tr>
</table>

<table>
<tr><th>FASI DI ATTUAZIONE</th><th>DESCRIZIONE DELLE FASI</th><th>MODULI CORRELATI</th><th>FUNZIONI AZIENDALI INTERESSATE</th></tr>
<tr>
<td>QUALIFICAZIONE DELLA VIOLAZIONE e contestuale valutazione della necessità di notificazione al Garante e comunicazione agli interessati</td>
<td>Il titolare con l'ausilio del DPO (ove nominato) e di altri soggetti quali ad es. l'amministratore di sistema, il referente dell'area in cui si è verificata la violazione, responsabile interno privacy, IT manager, consulenti, etc. deve valutare la portata del data breach in termini di impatto rispetto ai dati personali ed ai diritti e le libertà degli interessati.
Infatti, <u>soltanto nei casi in cui la violazione non presenta rischi per i diritti e per le libertà fondamentali delle persone interessate (e ciò è dimostrato) la notificazione al Garante (ed eventuale comunicazione agli interessati) non deve essere effettuata.</u>
Occorre pertanto che il soggetto individuato dal titolare (es. referente area in cui si è verificata la violazione, responsabile interno privacy, etc.) qualifichi la tipologia di violazione riscontrata seguendo le indicazioni riportate nella seguente tabella, che sarà poi oggetto di approvazione da parte del titolare e del DPO (ove presente):
<table>
<tr><th colspan="4">QUALIFICAZIONE VIOLAZIONE</th></tr>
<tr><td>Violazione di riservatezza: divulgazione o accesso a dati personali non autorizzato o accidentale</td><td>Violazione di integrità: alterazione di dati personali non autorizzata o accidentale</td><td>Violazione di disponibilità: perdita, inaccessibilità, o distruzione, accidentale o non autorizzata, di dati personali</td><td>Rischio assente</td></tr>
<tr><td>×</td><td>×</td><td>×</td><td>×</td></tr>
<tr><td>Motivazione:</td><td>Motivazione:</td><td>Motivazione:</td><td>Motivazione:</td></tr>
</table>
Note:
1. in particolari circostanze le violazioni potrebbero essere combinate tra loro.
2. in caso di sbarramento dell'ultima casella, non seguirà la notificazione al Garante (ed eventuale comunicazione agli interessati).</td>
<td>Tabella qualificazione violazione</td>
<td><u>Responsabile</u>:

TITOLARE DEL TRATTAMENTO
DPO (ove presente)</td>
</tr>
</table>

<table>
<tr><th>FASI DI ATTUAZIONE</th><th>DESCRIZIONE DELLE FASI</th><th>MODULI CORRELATI</th><th>FUNZIONI AZIENDALI INTERESSATE</th></tr>
<tr>
<td>VALUTAZIONE DEL RISCHIO e valutazione della necessità di comunicazione agli interessati</td>
<td>E' sufficiente un rischio "semplice" per far sorgere l'obbligo di notifica al garante, mentre è necessario un rischio "elevato" per far scaturire l'obbligo di comunicazione agli interessati.
Pertanto, il soggetto individuato dal titolare (possibilmente lo stesso soggetto che ha qualificato la violazione compilando l'apposita tabella), appurato che la violazione rappresenti un rischio per i diritti e le libertà delle persone fisiche, dovrà procedere alla valutazione del rischio, seguendo il seguente schema:
<table>
<tr><th>Descrizione violazione</th><th>Rischio semplice (solo notifica al Garante)</th><th>Rischio elevato (anche comunicazione agli interessati)</th></tr>
<tr><td>(XXXXX)</td><td>×</td><td></td></tr>
<tr><td>(YYYYY)</td><td></td><td>×</td></tr>
<tr><td>(ZZZZZZ)</td><td>×</td><td></td></tr>
</table>
Tale schema dovrà essere sottoposto all'approvazione del titolare e del DPO (ove presente).

Criteri per una valutazione accurata del livello di rischio:
1) Tipo di violazione
2) Natura, sensibilità e volume dei dati personali
3) Facilità di identificazione degli interessati attraverso i dati violati
4) Gravità delle conseguenze per le persone fisiche ad es. a livello di reputazione, etc
5) Categorie di interessati coinvolte (es. minori, etc)
6) Quantità di interessati coinvolti

Esempi di rischi "semplici" per i diritti e le libertà degli interessati conseguenti ad una violazione:
- 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).

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 (es. dati di localizzazione, finanziari, relativi alle abitudini e preferenze);
- comportare rischi imminenti e con un'elevata probabilità di accadimento (es. 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 (es. pazienti, minori, soggetti indagati).</td>
<td>Tabella valutazione del rischio</td>
<td><u>Responsabile:</u>
TITOLARE DEL TRATTAMENTO E DPO (ove presente)</td>
</tr>
<tr>
<td>NOTIFICAZIONE AL GARANTE</td>
<td>Il TITOLARE provvede alla notifica della violazione al Garante in modalità telematica (tramite posta elettronica certificata) e con sottoscrizione elettronica senza giustificato ritardo e, comunque, <u>entro 72 ore dal momento in cui ne è venuto a conoscenza</u> ovvero dal momento in cui è avvenuta la comunicazione da parte del Responsabile (o del soggetto che è venuto a conoscenza della violazione).

Il responsabile, sulla base di <u>specifica autorizzazione del titolare</u> <u>contrattualmente prevista</u>, può eseguire personalmente la notifica per conto di quest'ultimo.
Ad ogni modo, le responsabilità nei confronti dell'autorità e degli interessati scaturenti dalla notifica o dalla sua mancanza, permangano in capo al titolare, infatti in caso di negligenza, il responsabile potrà rispondere unicamente nei confronti del titolare.
Qualora la notifica all'Autorità di controllo <u>non sia effettuata entro 72 ore</u>, deve essere <u>corredata dai motivi del ritardo.</u></td>
<td>Modulo segnalazione violazione al garante</td>
<td><u>Responsabile:</u>

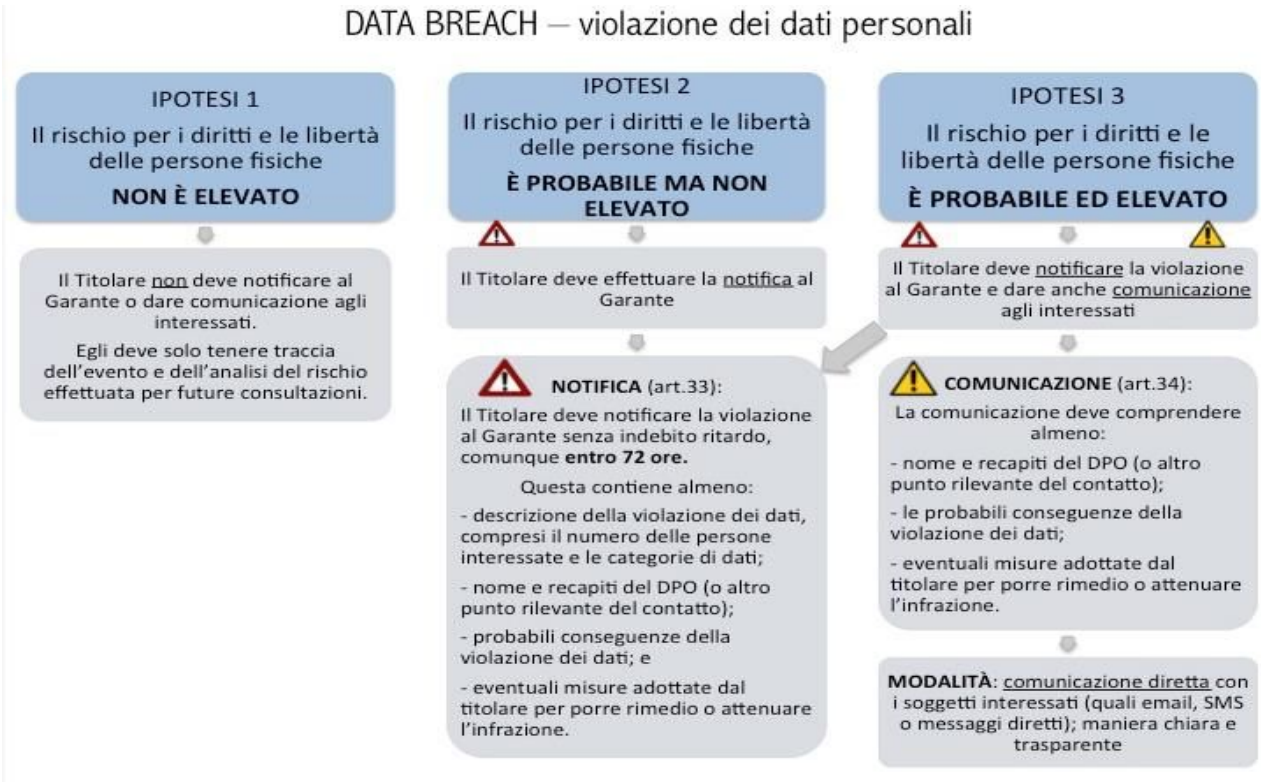
TITOLARE DEL TRATTAMENTO</td>
</tr>
</table>

FASI DI ATTUAZIONE	DESCRIZIONE DELLE FASI	MODULI CORRELATI	FUNZIONI AZIENDALI INTERESSATE
	Elementi utili a bilanciare le esigenze di celerità del messaggio con quelle di una sua sostanziale accuratezza e completezza: **1.** La prima tecnica è l'utilizzo dell'"approssimazione". Il titolare che non sia ancora in grado di conoscere con certezza il numero di persone e di dati personali interessati dalla violazione può comunicarne in prima battuta un ammontare approssimativo, provvedendo a specificare il numero esatto a seguito di accertamenti. **2.** Il secondo strumento è la "notificazione in fasi". In questo caso il titolare, per la complessità o estensione della violazione, potrebbe non essere in grado di fornire con immediatezza all'autorità tutte le informazioni necessarie. Potrà allora ottemperare agli obblighi di notifica comunicando, dopo una prima e rapida notifica di alert, tutte le informazioni per fasi successive, aggiornando di volta in volta l'autorità sui nuovi riscontri. **3.** Possibilità di notifica differita, dopo le 72 ore previste dall'art. 33 GDPR. È il caso in cui, per esempio, un'impresa subisca violazioni ripetute, ravvicinate e di simile natura che interessino un numero elevato di soggetti. Al fine di evitare un aggravio di oneri in capo al titolare e l'invio scaglionato di un numero elevato di notificazioni tra loro identiche, il titolare è autorizzato ad eseguire un'unica "notifica aggregata" di tutte le violazioni occorse nel breve periodo di tempo (anche se superi le 72 ore), purché la notifica motivi le ragioni del ritardo. **"Notifica per fasi":** che può essere adoperata dai Titolari nel caso di violazioni complesse (come nel caso di cyber attacchi alla sicurezza), per i quali è necessario realizzare delle indagini approfondite, i cui risultati verranno notificati in più "fasi" susseguenti, senza ingiustificato ritardo. In questi casi, quando il Titolare invia la notifica per la prima volta all'Autorità, deve informarla contestualmente del fatto che fornirà ulteriori informazioni successivamente, in quanto sono in corso indagini approfondite. L'Autorità competente dovrebbe infatti essere d'accordo sulle modalità e le tempistiche con cui tali ulteriori informazioni saranno notificate nelle fasi successive. Inoltre, se dalle indagini approfondite, dovesse risultare che il data breach è stato contenuto e che nessuna violazione si è verificata, tale informazione deve essere aggiunta nelle notifiche successive alla prima. Non è infatti prevista alcuna sanzione per avere notificato all'autorità una violazione che risulta in seguito come mai avvenuta.		
COMPILAZIONE MODULO DI SEGNALAZIONE (in caso di notificazione al Garante)	Il Titolare, con l'ausilio del DPO (ove nominato) individua il soggetto che compila il modulo (es. amministratore di sistema, referente area coinvolta dalla violazione dei dati, responsabile interno privacy) e le relative tempistiche. Nel modulo da notificare al Garante occorre indicare: a) 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) 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) descrizione delle probabili conseguenze della violazione dei dati personali; d) 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. Qualora e nella misura in cui non sia possibile fornire le suddette informazioni contestualmente, le stesse possono essere fornite in fasi successive, senza ulteriore ingiustificato ritardo. Il modulo deve essere redatto utilizzando un linguaggio semplice e chiaro e deve contenere un'accurata descrizione della natura della violazione dei dati personali, nonché suggerimenti e raccomandazioni su come poter attenuare i potenziali effetti negativi derivanti dalla violazione dei dati personali. In altre parole, occorre procedere ad una descrizione completa ed esaustiva dell'infrazione. **Esempi di "categorie di interessati":** minori o soggetti vulnerabili, persone con disabilità, lavoratori, clienti, fornitori, etc.	**Modulo segnalazione violazione al garante**	**Responsabile:** **TITOLARE DEL TRATTAMENTO E DPO (ove presente)**

FASI DI ATTUAZIONE	DESCRIZIONE DELLE FASI	MODULI CORRELATI	FUNZIONI AZIENDALI INTERESSATE
COMUNICAZIONE AGLI INTERESSATI (in caso di rischio elevato)	Il titolare del trattamento con l'ausilio del DPO (ove nominato) individua il soggetto (es. amministratore di sistema, referente area coinvolta dalla violazione dei dati, responsabile privacy interno) che si occuperà della comunicazione anche a ciascuno degli interessati coinvolti dalla violazione, senza ingiustificato ritardo (contestualmente alla notificazione al Garante o subito dopo e, comunque, entro 72 ore dalla scoperta della violazione), al fine di consentirgli di adottare idonee precauzione volte a ridurre al minimo il potenziale danno derivante dalla violazione dei suoi dati personali. Il titolare, con l'ausilio del DPO (ove nominato), valuterà la correttezza e completezza del contenuto della comunicazione prima che la stessa venga inoltrata. Le informazioni da fornire a ciascun interessato coincidono con quelle da fornire al Garante; in particolare, la suddetta comunicazione deve descrivere con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contenere almeno le informazioni e le misure indicate sopra *sub* lettera b), c) e d). L'adeguatezza della comunicazione è determinata non solo dal contenuto del messaggio, ma anche dalle modalità di effettuazione. Il messaggio dovrebbe essere comunicato in maniera evidente e trasparente, evitando quindi di inviare le informazioni nel contesto di *update* o *newsletter*, che potrebbero essere facilmente fraintesi dai lettori. Devono pertanto essere privilegiate modalità di comunicazione diretta con i soggetti interessati (e-mail, sms, messaggi diretti, etc.). Inoltre, occorre considerare possibili formati alternativi di visualizzazione del messaggio e delle diversità linguistiche dei soggetti riceventi (es. l'utilizzo della lingua madre dei soggetti riceventi rende il messaggio immediatamente comprensibile). **Possibili modalità di comunicazione a ciascun interessato:** - comunicazione diretta: e-mail, sms, notifiche; - comunicazione pubblica (nel caso in cui la prima modalità di comunicazione comporti un impegno sproporzionato): es banner sul website; - in modo accessibile per tutti gli interessati: es. prevedere traduzione in più lingue	**E-mail, sms, messaggi diretti**	**Responsabile:** **TITOLARE DEL TRATTAMENTO E DPO (ove presente)**
ESCLUSIONE OBBLIGO COMUNICAZIONE AGLI INTERESSATI	Il **TITOLARE** non è tenuto alla comunicazione all'interessato se è soddisfatta almeno 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 ad esempio 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; c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede con una comunicazione pubblica o con una misura simile, tramite la quale gli interessati sono informati con analoga efficacia. Nel caso in cui il titolare del trattamento non comunichi 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.		**Responsabile:** **TITOLARE DEL TRATTAMENTO**
ARCHIVIAZIONE DELLE VIOLAZIONI	Il titolare (con l'ausilio del DPO ove presente) deve documentare tutte le violazioni che si siano verificate, indipendentemente dall'obbligo di notifica, al fine di poter dimostrare la conformità al GDPR del trattamento effettuato. Il titolare individua il soggetto (es. responsabile interno privacy, amministratore di sistema, etc.) che si occuperà della registrazione dei dati relativi alla violazione, comprese le circostanze in cui la stessa si è verificata, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Spetta al titolare determinare un periodo appropriato di conservazione del registro (es. 2 anni); in ogni caso, il registro dovrà essere liberamente accessibile e consultabile da parte del DPO, ove presente, nonché da parte dell'Autorità di controllo per le opportune verifiche. Nel registro, il titolare dovrà pertanto raccogliere tutte le violazioni di dati personali che hanno coinvolto l'Organizzazione e dunque: a) violazioni oggetto di notificazione al Garante e relativo riscontro; b) violazioni oggetto di comunicazione agli interessati e relativo riscontro; c) violazioni non notificate al Garante e/o non comunicate agli interessati e relativa motivazione.	**Registro delle violazioni**	**Responsabile:** **TITOLARE DEL TRATTAMENTO E DPO (ove presente)**

FASI DI ATTUAZIONE	DESCRIZIONE DELLE FASI	MODULI CORRELATI	FUNZIONI AZIENDALI INTERESSATE
SANZIONI PREVISTE	In caso di mancato rispetto degli obblighi previsti in materia di Data Breach, il Regolamento GDPR prevede sanzioni pecuniarie fino a 10.000.000 euro o per le imprese fino al 4% del fatturato mondiale annuo dell'esercizio precedente, se superiore. In particolare, sono previste le seguenti sanzioni amministrative: • in caso di mancata o ritardata comunicazione al Garante: da 25mila a 150mila euro; • in caso di omessa o mancata comunicazione agli utenti: da 150 euro a 1000 euro per ogni società, ente o persona interessata; • in caso di mancata tenuta dell'inventario delle violazioni aggiornato: da 20mila a 120mila euro.		

SCHEMA DI SINTESI



REGISTRAZIONI

CODICE	REGISTRAZIONE
MSVG	Modulo segnalazione violazione al Garante
MCD	E-mail, SMS, messaggi diretti
TQV	Tabella Qualificazione violazione
TVR	Tabella valutazione del rischio
RV	Registro delle violazioni

RESPONSABILITA'

FUNZIONE	RESPONSABILE	COINVOLTO
Titolare del trattamento	x	
DPO		x
Responsabile/incaricato del trattamento oggetto di violazione		x
Responsabile interno privacy		x
Amministratore di sistema		X
Responsabile IT		X
Responsabili di area		X

ALLEGATO: MODULO SEGNALAZIONE VIOLAZIONE AL GARANTE

ALL'AUTORITÀ GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

N.B. spedire per posta elettronica certificata

Notifica di violazione dei dati personali (data breach) ai sensi dell'art. 33 del regolamento generale sulla protezione dei dati

Il sottoscritto responsabile del trattamento _____, a nome e per conto della azienda (dare le coordinate – ragione sociale, indirizzo)
Notifica di seguito la avvenuta violazione di dati personali, i cui tempi e modalità sono di seguito descritti in dettaglio

Art. 33 - comma 1

data ed ora della presente notifica _____

data ed ora in cui il responsabile del trattamento è venuto a conoscenza della violazione ____

data ed ora in cui la violazione si è verificata (se diversa dalla data precedente e se i dati sono disponibili) _____

NB- ove la notifica non sia stata effettuata entro 24 ore, compilare il campo sottostante
Si precisa che la notifica non è stata effettuata entro le 24 ore da quando il responsabile ne è venuto a conoscenza per i seguenti giustificati motivi[1]

_____

_____

Art 33 – comma 2

Si precisa che l'incaricato del trattamento _____ ha allertato ed informato il responsabile del trattamento immediatamente dopo aver accertato la violazione, in data____ alle ore ____, con comunicazione
□ verbale,
□ scritta (dare estremi identificativi della comunicazione, se disponibili))

Art 33 – comma 3, lettera a)

a.1 Descrizione della natura della violazione dei dati personali[2]

_____

_____

a.2 Descrizione delle categorie e il numero di interessati in questione e le categorie e il numero di registrazioni dei dati in questione

_____

_____

a.3 Descrizione delle categorie di dati personali[3]

_____
_____

a.4 Numero di interessati in questione[4]

---

[1] Si raccomanda di compilare in modo assai dettagliato questo campo, per evitare che l'autorità Garante possa avviare una procedura per infrazione dei tempi massimi di notifica all'autorità Garante. Una violazione di questo tipo comporta sanzioni piuttosto significative ed è bene che le motivazioni vengano giustificate in ampio dettaglio, offrendo ogni possibile documentazione di supporto e convalida.

[2] Per meglio consentire all'autorità Garante di comprendere la modalità di violazione, è bene premettere una sintetica illustrazione della architettura del sistema di trattamento informatico o manuale, che è stato oggetto di violazione.
A titolo puramente esemplificativo, il titolare del trattamento potrà illustrare il luogo in cui si è verificata la violazione dei dati, se la violazione ai dati è avvenuta a seguito di smarrimento di dispositivi portatili di supporto, oppure di violazione deliberata da parte di soggetti criminosi terzi, quale specifico tipo di violazione si sia verificata, ad esempio una lettura dei dati non autorizzata, che fa presumere che i dati non siano stati copiati, oppure una copia abusiva dei dati, che sono ancora presenti sul sistema di trattamento, oppure una asportazione dei dati, di cui non esiste più copia, oppure una alterazione, che fa sì che i dati siano presenti nel sistema di trattamento ma non siano affidabili, oppure una cancellazione di dati, che possono o meno essere ripristinabili, in funzione della disponibilità di copie di backup. Se possibile, dovranno essere indicati anche che i nomi dei soggetti che si ritiene possano essere stati coinvolti nella violazione, almeno in via ipotetica.
A completamento di questa illustrazione, sarà bene descrivere in dettaglio i supporti sui quali si trovavano i dati oggetto della violazione; tali supporti possono evidentemente essere di tipo informatico fisso, di tipo informatico mobile, di tipo cartaceo od altro.
Segnalare anche il fatto che la violazione potrebbe coinvolgere anche interessati di altri paesi europei, per allertare le appropriate autorità nazionali.

3 Nei limiti del possibile, sarà bene dare una illustrazione alquanto articolata della natura dei dati violati, per permettere l'autorità Garante di effettuare una rapida valutazione della gravità della situazione. Appare evidente che una violazione di dati afferenti alla salute è potenzialmente più grave di una violazione afferente a dati anagrafici, magari reperibili con relativa facilità sugli elenchi pubblici. Alla luce delle considerazioni esposte in precedenza, occorre anche mettere in evidenza se questi dati possono o meno essere utilizzati per furti di identità, con le possibili drammatiche conseguenze. Si dovrà anche mettere in evidenza, nel descrivere la natura dei dati, se l'eventuale furto di identità può avere anche gravi e dirette ripercussioni economiche, come ad esempio avviene quando è stato sottratto un PIN ed i dati di una tessera bancomat, usando gli ormai ben noti dispositivi di alterazione criminosa delle macchine ATM.

4 In molti casi non è possibile individuare con esattezza il numero degli interessati, i cui dati sono stati violati. Laddove possibile, indicare il numero approssimato, se è possibile fare queste ipotesi, oppure articolare in modo quanto più dettagliato possibile la categoria degli interessati coinvolti, per permettere all'autorità Garante di effettuare una valutazione appropriata. Ad esempio, nel caso i dati personali violati siano stati catturati presso un ATM modificato da criminali, si dovrà indicare l'ora presumibile nella quale l'apparato è stato alterato, tipicamente nelle prime ore della sera del venerdì, sino alla ora nella quale la alterazione è stata individuata. Successivamente si potranno anche fornire elenchi dettagliati

_____

_____

a.5 Descrizione delle categorie e il numero di registrazioni dei dati in questione

_____

_____

Art 33 – comma 3, lettera b)

b.1 Identità e le coordinate di contatto del responsabile della protezione dei dati, o di altro punto di contatto presso cui ottenere più informazioni (dare anche n. di cellulare ed ogni altra indicazione utile per un immediato contatto da parte della autorità Garante, ad esempio dare contatti afferenti all'incaricato ed al responsabile della protezione dei dati personali)

_____

Art 33 – comma 3, lettera c)

c.1 Descrizione delle conseguenze della violazione dei dati personali (indicare le conseguenze effettive ed anche quelle ragionevolmente prevedibili)[5]

_____

_____

Art 33 – comma 3, lettera d)

d.1 Descrizione delle misure proposte o adottate dal responsabile del trattamento per porre rimedio alla violazione dei dati personali[6]

_____

_____

Art. 33 – comma 4

Dare adeguata motivazione ed offrire ogni possibile dettagli in merito

Art 33 – comma 5

Il titolare del trattamento dichiara che presso di lui è disponibile tutta la documentazione afferente alla violazione dei dati personali, incluse le circostanze in cui si è verificata, le sue conseguenze e i provvedimenti adottati per porvi rimedio.
Il titolare del trattamento dichiara altresì che la documentazione è tale da consentire all'autorità di controllo di verificare il rispetto del disposto dell'articolo 33.
In essa figurano unicamente le informazioni necessarie a tal fine. Ovviamente, si resta a disposizione per fornire ulteriori informazioni, atte a soddisfare i criteri ed i requisiti concernenti l'accertamento della violazione di dati personali di cui ai commi 1 e 2 e le circostanze particolari in cui il responsabile del trattamento e l'incaricato del trattamento sono tenuti a notificare la violazione.

degli interessati coinvolti, estraendo i dati dalla memoria della macchina ATM. Ove invece sia stato alterato in modo criminoso un POS, può essere estremamente difficile individuare la data nella quale la alterazione è avvenuta ed occorre quindi assumere un atteggiamento oltremodo prudenziale, risalendo assai indietro nel tempo.

[5] Appare evidente che una indicazione dettagliata delle possibili conseguenze della violazione, già anticipata in una porzione precedente della notifica, rappresenta un elemento fondamentale di valutazione della gravità della situazione, da parte dell'autorità Garante, sia a livello nazionale, sia a livello di altre autorità nazionali, potenzialmente coinvolte.

[6] È evidente che una descrizione delle misure già adottate è assai più interessante, rispetto ad una descrizione delle misure che si intendono adottare. In quest'ultimo caso, occorre comunque sempre indicare un tempo limite entro il quale le misure in questione saranno adottate. Si raccomanda al compilatore della notifica di prestare attenzione al fatto che spesso vi possono essere dei problemi di natura economica, a finanziamento delle iniziative proposte, che potrebbero sfuggire al campo di responsabilità diretto. In questo caso, occorre avanzare una precisazione specifica.