REGIONE MARCHE
CONSIGLIO - ASSEMBLEA LEGISLATIVA

DELIBERA N.	438
SEDUTA N.	154
DATA	23/04/2024

LEGISLATURA N. XI

Oggetto: **PROCEDURA DI GESTIONE DELLE VIOLAZIONI DEI DATI PERSONALI**

Il 23 aprile 2024 si è riunito presso la sala adiacente all'aula del Assemblea legislativa regionale, in via Tiziano n. 44, ad Ancona l'Ufficio di presidenza regolarmente convocato.

		PRESENTI	ASSENTI
Dino Latini	- Presidente	X	
Gianluca Pasqui	- Vicepresidente	X	
Andrea Biancani	- Vicepresidente	X	
Pierpaolo Borroni	- Consigliere segretario	X	
Micaela Vitri	- Consigliere segretario	X	

Essendosi in numero legale per la validità dell' adunanza assume la presidenza il Presidente dell'Assemblea legislativa delle Marche **Dino Latini** che dichiara aperta la seduta alla quale assiste il Segretario dell'Ufficio di presidenza **Antonio Russi** .

LA DELIBERAZIONE IN OGGETTO E' APPROVATA ALL'UNANIMITA' DEI PRESENTI

PUBBLICATA NEL BURM N. DEL

OGGETTO: Procedura di gestione delle violazioni dei dati personali

L'Ufficio di Presidenza

VISTO il documento istruttorio riportato nella presente deliberazione;

RITENUTO, per i motivi indicati in tale documento istruttorio, di deliberare in merito;

VISTO l'articolo 15, comma 1, lettera h), del regolamento interno di organizzazione e funzionamento dell'Assemblea legislativa regionale delle Marche;

VISTA la proposta della dirigente del Servizio Affari legislativi e coordinamento Commissioni assembleari, che contiene il parere favorevole sotto il profilo della legittimità e della regolarità tecnica previsto dall'articolo 3, comma 3, della legge regionale 30 giugno 2003, n. 14 (Riorganizzazione della struttura amministrativa del Consiglio Regionale) e la dichiarazione di insussistenza di situazioni anche potenziali di conflitto di interessi, nonché l'attestazione della stessa che dalla presente deliberazione non deriva e non può derivare alcun impegno di spesa a carico del bilancio del Consiglio-Assemblea legislativa regionale;

Con la votazione, resa in forma palese, riportata a pagina 1;

DELIBERA

di approvare, con riferimento al Consiglio - Assemblea legislativa delle Marche, la procedura di gestione delle violazioni dei dati personali e il relativo modello di verbale contenuti rispettivamente negli allegati A e B alla presente deliberazione, che costituiscono parte integrante della stessa.

Il Presidente dell'Assemblea legislativa regionale
(Dino Latini)

Il Segretario dell'Ufficio di presidenza
(Antonio Russi)

DOCUMENTO ISTRUTTORIO

Il regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), ha stabilito nuovi obblighi a carico delle amministrazioni pubbliche. L'articolo 4 di tale regolamento, in particolare, ha definito

L'articolo 4 di tale regolamento, in particolare, ha definito "dato personale" qualsiasi informazione riguardante una persona fisica identificata o identificabile, aggiungendo che 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, e "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. Ha definito, inoltre, come "violazione dei dati personali" 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.

L'articolo 32 ha stabilito che, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso, la pseudonimizzazione e la cifratura dei dati personali; la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento, come pure di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico, nonché una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento. Ha disposto poi che, nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati e che il titolare e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

L'articolo 33 ha previsto, in caso di violazione dei dati personali, l'obbligo per il titolare del trattamento di notificare la violazione 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 sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche e, qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, di corredarla dei motivi del ritardo. Ha imposto, inoltre, al responsabile del trattamento di informare il titolare senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione. Ha stabilito, poi, che la notifica deve almeno 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; 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; descrivere le probabili conseguenze della violazione dei dati personali e le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla stessa e anche, se del caso, per attenuarne i possibili effetti negativi. Ha disposto che, 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 e, infine, che il titolare del trattamento deve documentare qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le conseguenze e i provvedimenti adottati per porvi rimedio.

L'articolo 34 ha imposto al titolare del trattamento di comunicare la violazione all'interessato senza ingiustificato ritardo quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche e ha stabilito che tale comunicazione deve descrivere con un linguaggio semplice e chiaro la natura della medesima violazione e contenere almeno il nome e i dati di contatto del

responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni; descrivere le probabili conseguenze della violazione dei dati personali; le misure adottate o di cui si propone l'adozione da parte del titolare per porre rimedio alla stessa violazione e anche, se del caso, per attenuarne i possibili effetti negativi. Ha escluso, invece, l'obbligo di comunicazione se è soddisfatta una delle condizioni definite e, cioè, se 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; se ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati; se la comunicazione richiederebbe sforzi sproporzionati. Ha previsto che, in tal caso, si procede a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia. Ha disposto poi che, 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 esclusione dall'obbligo di comunicazione sia soddisfatta.

Specifiche indicazioni in merito alla violazione dei dati personali sono state fornite dal Gruppo di lavoro istituito dall'articolo 29 della direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati. Il medesimo Gruppo, che fino al 25 maggio 2018 ha avuto, tra l'altro, il compito di esaminare ogni questione attinente all'applicazione delle norme nazionali di attuazione per contribuire alla loro applicazione omogenea, il 3 ottobre 2017, ha adottato le "Linee guida sulla notifica delle violazioni di dati personali ai sensi del regolamento (UE) 2016/679" e le ha modificate il 6 febbraio 2018.

Il Comitato europeo per la protezione dei dati o European Data Protection Board (EDPB), istituito dal regolamento (UE) 2016/679, inoltre, il 14 dicembre 2021 ha adottato le "Linee guida 01/2021 su esempi riguardanti la notifica di una violazione dei dati personali" e il 28 marzo 2023 ha adottato le "Linee guida 9/2022 sulla notifica delle violazioni dei dati personali ai sensi del RGPD", che hanno sostituito le precedenti.

L'Agenzia europea per la sicurezza delle reti e dell'informazione, istituita dal regolamento (CE) n. 460/2004 del Parlamento europeo e del Consiglio, del 10 marzo 2004, ha pubblicato, a dicembre 2013, "Raccomandazioni per una metodologia di valutazione della gravità delle violazioni dei dati personali".

L'Agenzia dell'Unione europea per la cibersicurezza o European Union Agency for Network and Information Security (ENISA), istituita dal regolamento (UE) 17 aprile 2019, n. 2019/881/UE del Parlamento europeo e del Consiglio ha fornito ulteriori indicazioni.

Rispetto all'ordinamento interno, il decreto legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE", come modificato dal decreto legislativo 10 agosto 2018, n. 101 "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)" ha dato attuazione al regolamento (UE) n. 2016/679.

Alcuni provvedimenti dell'Autorità Garante per la protezione dei dati personali hanno fornito ulteriori indicazioni rispetto alla procedura di gestione delle violazioni dei dati personali.

Secondo quanto previsto da tali atti e al fine di assicurare un più completo adeguamento alla normativa dell'Unione europea e statale, è stata predisposto il testo che disciplina la gestione delle violazioni dei dati personali nell'ambito del Consiglio- Assemblea legislativa delle Marche.

Per la stesura ci si è avvalsi del supporto del Responsabile della protezione dei dati personali.

La responsabile del procedimento
(Elisa Moroni)

PROPOSTA E PARERE DEL DIRIGENTE DEL SERVIZIO
AFFARI LEGISLATIVI E COORDINAMENTO COMMISSIONI ASSEMBLEARI

La sottoscritta propone all'Ufficio di presidenza l'adozione della presente deliberazione in merito alla quale esprime parere favorevole sotto il profilo della legittimità e della regolarità tecnica. Visti, inoltre, l'articolo 6 bis della legge 7 agosto 1990, n. 241 (Nuove norme sul procedimento amministrativo), nonché gli articoli 6 e 7 del decreto del Presidente della Repubblica 16 aprile 2013, n. 62 (Regolamento recante codice di comportamento dei dipendenti pubblici a norma dell'articolo 54 del decreto legislativo 30 maggio 2001, n.165), dichiara, ai sensi dell'articolo 47 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 (Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa), che, in relazione alla presente deliberazione, non si trova in situazione anche potenziale di conflitto di interessi. Attesta, inoltre, che dalla presente deliberazione non deriva e non può derivare alcun impegno di spesa a carico del bilancio del Consiglio-Assemblea legislativa regionale.

La dirigente del Servizio Affari legislativi e
coordinamento Commissioni assembleari
(Elisa Moroni)

La presente deliberazione si compone di 10 pagine, di cui n. 5 pagine di allegati che formano parte integrante della stessa.

Il Segretario dell'Ufficio di presidenza
Antonio Russi

Allegato A

PROCEDURA DI GESTIONE DELLE VIOLAZIONI DEI DATI PERSONALI RELATIVA AL CONSIGLIO - ASSEMBLEA LEGISLATIVA DELLE MARCHE, DI SEGUITO INDICATO COME "CONSIGLIO"

1. Definizione e tipologie di violazione dei dati personali

1.1. Si definisce "violazione dei dati personali" 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. Si tratta di un incidente di sicurezza, in conseguenza del quale non si è più in grado di garantire l'osservanza dei principi relativi al trattamento dei dati personali di cui all'articolo 5 del regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

1.2. Una violazione dei dati personali può essere classificata in base ai seguenti tre principi:

- violazione della riservatezza: si verifica in caso di divulgazione dei dati personali o accesso agli stessi in modo non autorizzato o accidentale;
- violazione dell'integrità: si verifica in caso di modifica non autorizzata o accidentale dei dati personali;
- violazione della disponibilità: si verifica in caso di perdita, accesso o distruzione accidentale o non autorizzata di dati personali. Essa può essere temporale se i dati personali sono recuperabili, ma è necessario un certo periodo di tempo; ovvero permanente se i dati personali non possono essere recuperati.

2 Analisi del rischio (probabile e/o elevato) per i diritti e delle libertà di un soggetto interessato

2.1. L'articolo 33, paragrafo 1, del regolamento stabilisce che, in caso di violazione dei dati personali, il titolare del trattamento notifica la violazione 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 sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche e che, qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

L'articolo 34, paragrafo 1, del regolamento chiarisce che, quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.

2.2. L'analisi del rischio per i diritti e le libertà dell'interessato deve essere svolta secondo i seguenti due parametri:

a) probabilità delle conseguenze della violazione per l'interessato, al fine, in caso di esito positivo, di procedere alla notifica di tale evento al Garante per la protezione dei dati personali, di seguito indicato come "Garante";
b) gravità delle conseguenze della medesima violazione per l'interessato, al fine, in caso di esito positivo, di effettuare la comunicazione della violazione allo stesso.

2.3. Dei due esiti, ossia gravità e probabilità, il secondo è autonomamente sufficiente a determinare l'obbligo di notifica al Garante e prescinde da una valutazione in ordine alla severità delle conseguenze pregiudizievoli per l'interessato. Pertanto il titolare (o contitolare) del trattamento, nel periodo di reazione ad una violazione, deve, innanzitutto, concentrare le sue risorse di analisi sulla determinazione della probabilità del rischio, e immediatamente dopo, in caso di rischio probabile, anche sulla comprensione della sua gravità.

2.4 Le conseguenze pregiudizievoli che potrebbero derivare dalla violazione e che vanno valutate in termini di probabilità e di gravità sono quelle elencate nei Considerando n. 75 e 85 del regolamento. Tale valutazione (oggettiva) del rischio va condotta tenendo conto dei seguenti fattori:

- tipologia della violazione;
- natura, carattere sensibile e volume dei dati personali;
- facilità di identificazione della persona fisica;
- gravità delle conseguenze per la persona fisica;
- caratteristiche particolari dell'interessato. Sussiste un rischio più elevato di danno se la violazione riguarda dati personali relativi a minori o ad altre persone fisiche vulnerabili;
- caratteristiche particolari del titolare (o contitolare) del trattamento: la natura ed il ruolo di tale soggetto e delle sue attività può influire sul livello di rischio per le persone fisiche a seguito di una violazione;

- numero di persone fisiche interessate: di norma, maggiore è il numero delle persone fisiche interessate, maggiore è l'impatto che una violazione può avere.

3. Cosa fare in caso di violazione

3.1 Il soggetto interno al Consiglio che subisce, rileva o viene a conoscenza di una violazione, deve effettuare una segnalazione scritta al Segretario generale o al dirigente interessato, ovvero al responsabile della protezione dei dati personali. Tale segnalazione deve essere trasmessa mediante posta elettronica al relativo indirizzo istituzionale o di posta certificata, oppure consegnata a mano ai medesimi soggetti.

3.2 La segnalazione deve contenere, almeno, le seguenti informazioni:

- descrizione della violazione (anche potenziale);
- modalità con la quale si è avuta conoscenza della violazione;
- dati personali oggetto di violazione;
- ogni altro elemento riguardante la violazione.

4. Notifica della violazione al Garante

4.1. Il titolare (o contitolare) del trattamento deve notificare la violazione dei dati personali senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, nel caso in cui l'esito dell'analisi del rischio abbia rilevato una probabilità di rischio per i diritti e le libertà degli interessati coinvolti nell'evento.

Tale termine decorre dal momento in cui il titolare (o contitolare) del trattamento è ragionevolmente certo che si è verificato un incidente di sicurezza che ha portato alla compromissione dei dati personali: dunque, il titolare (o contitolare) del trattamento è tenuto a prendere le misure necessarie per assicurarsi di venire a conoscenza di eventuali violazioni in maniera tempestiva, in modo da poter adottare le misure appropriate.

4.2. La notifica della violazione al Garante deve almeno contenere le seguenti informazioni:

- descrizione della natura della violazione dei dati personali inclusi, ove possibile, le categorie e il numero, anche approssimativo, degli interessati, nonché le categorie e il numero, anche approssimativo, dei relativi dati personali;
- nome e dati di contatto del responsabile della protezione dei dati personali o di un altro punto di contatto presso cui il Garante può ottenere informazioni;
- descrizione delle probabili conseguenze della violazione;
- descrizione delle misure adottate o di cui si propone l'attuazione per porre rimedio alla violazione dei dati occorsa ed eventualmente per attenuare i possibili effetti negativi.

La notifica deve essere inviata al Garante tramite l'apposita procedura telematica.

4.3. A seconda della natura della violazione, il titolare (o contitolare) del trattamento può avere la necessità di effettuare ulteriori accertamenti per stabilire tutti i fatti pertinenti la violazione. A tale fine, l'articolo 33, paragrafo 4, del regolamento acconsente alla notifica per fasi. Se, dopo la notifica, una successiva indagine dimostra che l'incidente di sicurezza è stato contenuto e che non si è verificata alcuna violazione, il titolare (o contitolare) del trattamento può informare il Garante. Queste informazioni possono, quindi, essere aggiunte alle informazioni già fornite e l'incidente può essere, di conseguenza, registrato come un evento che non costituisce una violazione.

4.4. Qualora non sia effettuata entro 72 ore, la notifica al Garante deve essere corredata dei motivi del ritardo.

5. Comunicazione all'interessato

5.1. Se la violazione ha prodotto un rischio elevato per i diritti e le libertà dell'interessato, il titolare (o contitolare) del trattamento deve effettuare, senza ingiustificato ritardo, ossia il prima possibile, la comunicazione della violazione a ciascun interessato.

L'obiettivo principale della comunicazione agli interessati è fornire loro informazioni specifiche sulle misure che questi possono prendere per proteggersi da eventuali conseguenze negative derivanti dalla violazione dei loro dati personali.

5.2. Nel rispetto del combinato disposto dell'articolo 33, paragrafo 2, e dell'articolo 34, paragrafo 2, del regolamento, il titolare (o contitolare) del trattamento deve fornire, con un linguaggio semplice e chiaro, almeno le seguenti informazioni:

- descrizione della natura della violazione;

- nome e dati di contatto del responsabile della protezione dei dati personali o di un altro punto di contatto presso cu l'interessato può ottenere informazioni;
- descrizione delle (probabili) conseguenze della violazione;
- descrizione delle misure adottate o di cui si propone l'adozione, da parte del titolare (o contitolare) del trattamento per porre rimedio alla violazione e anche, se del caso, per attenuarne i possibili effetti negativi.

5.3. In linea di principio, la violazione dovrebbe essere comunicata direttamente agli interessati coinvolti, a meno che ciò richieda uno sforzo sproporzionato. In tale caso si può procedere a una comunicazione pubblica o a una misura simile che permetta di informare gli interessati con analoga efficacia.
Nel comunicare una violazione si devono utilizzare messaggi dedicati che non devono essere inviati insieme ad altre informazioni. Deve essere scelto un mezzo che massimizzi la possibilità di comunicare correttamente le informazioni a tutti gli interessati.
5.4. In via generale, sussiste un rischio elevato quando la violazione può comportare un danno fisico, materiale o immateriale per le persone fisiche i cui dati sono stati violati.
Al riguardo l'Agenzia europea per la sicurezza delle reti e dell'informazione, a dicembre 2013, ha pubblicato "Raccomandazioni per una metodologia di valutazione della gravità di violazioni dei dati particolari". Tale metodologia è sintetizzata nella tabella che segue:

Gravità BASSA	L'interessato potrebbe incontrare alcuni inconvenienti, superabili senza problemi (ad esempio il tempo speso per reinserire le informazioni; fastidi; irritazione).
Gravità MEDIA	L'interessato potrebbe incontrare disagi significativi che sarà in grado di superare nonostante alcune difficoltà (ad esempio i costi aggiuntivi; rifiuto di accesso a servizi aziendali; mancanza di comprensione; stress; disturbi fisici minori).
Gravità ALTA	L'interessato potrebbe incontrare conseguenze significative che dovrebbe essere in grado di superare anche se con gravi difficoltà (ad esempio un'appropriazione indebita di fondi; inserimento in una black list; danni alla proprietà; perdita del lavoro; mandato di comparizione; peggioramento della salute).
Gravità MOLTO ALTA	L'interessato potrebbe incontrare un danno significativo o irreversibile (ad esempio la difficoltà finanziarie, come debiti ingenti; incapacità lavorativa; disturbi psicologici o fisici a lungo termine; morte).

6. Contitolare del trattamento
L'eventuale accordo di contitolarità deve includere disposizioni che stabiliscano chi, tra il titolare e il contitolare, è responsabile del rispetto degli obblighi di notifica delle violazioni.

7. Responsabile del trattamento
7.1. Sebbene il titolare (o contitolare) del trattamento conservi la responsabilità generale per la protezione dei dati personali, il responsabile del trattamento svolge un ruolo importante nel consentire al titolare (o contitolare) di adempiere ai propri obblighi, segnatamente in materia di notifica e comunicazione di una violazione.
Se il responsabile del trattamento viene a conoscenza di una violazione dei dati personali che sta trattando per conto del titolare (o contitolare) del trattamento, deve notificarla al titolare (o contitolare) del trattamento senza ingiustificato ritardo.
Il responsabile del trattamento non è tenuto a valutare la probabilità del rischio derivante dalla violazione prima di notificarlo al titolare (o contitolare) del trattamento; il primo deve, infatti, soltanto stabilire se si è verificata una violazione e, quindi, notificarla al titolare del trattamento.
7.2. Il responsabile del trattamento può effettuare la notifica per conto del titolare (o contitolare) del trattamento qualora quest'ultimo gli abbia concesso l'opportuna autorizzazione e ciò faccia parte degli accordi

contrattuali tra il titolare (o contitolare) del trattamento ed il responsabile del trattamento. La responsabilità legale della notifica rimane in capo al titolare (o contitolare) del trattamento.

8. Documentazione della violazione

8.1 Indipendentemente dal fatto che una violazione dei dati personali debba o meno essere notificata al Garante ed eventualmente comunicata agli interessati, il titolare (o contitolare) del trattamento deve conservare la documentazione di tutte le violazioni.

8.2 Il titolare (o contitolare) del trattamento è tenuto a registrare i dettagli di ciascuna violazione, comprese le cause, i fatti, i dati personali, gli effetti e le conseguenze della violazione, i relativi provvedimenti adottati per porvi rimedio, nonché il ragionamento alla base delle decisioni prese in conseguenza di una violazione.

9. Esempi di violazione

Possono risultare di particolare utilità, ai fini della valutazione pratica della necessità di notificare o meno al Garante e comunicare a ciascun interessato, le “Linee Guida n. 1/2021 su esempi riguardanti la notifica di una violazione dei dati personali”, adottate il 14 dicembre 2021 dal Comitato europeo per la protezione dei dati o european data protection board (EDPB).

Allegato B

Modello di verbale relativo alla violazione dei dati personali

Nome e cognome del verbalizzante	
Eventuali soggetti terzi (es. fornitori), coinvolti, a vario titolo, nella violazione	
Descrizione della violazione	
Strumenti informatici/parzialmente informatici/non informatici coinvolti nella violazione	
Tipologie di dati personali oggetto di violazione	
Categorie di soggetti interessati coinvolti nella violazione	
Data e ora (anche presunta) della violazione	
Data e ora di presa di conoscenza della violazione	
Data e ora di inizio della gestione della violazione	
Data e ora di conclusione della gestione della violazione	
Documentazione acquisita in merito alla violazione	
Descrizione delle attività tecniche/organizzative eseguite per mitigare la violazione	
Descrizione dei possibili effettivi negativi della violazione sui diritti e le libertà dei soggetti interessati coinvolti nella violazione	
Descrizione dei possibili effetti negativi della violazione sul Consiglio - Assemblea legislativa delle Marche	
Descrizione delle attività svolte (o che si intende svolgere) per ridurre il rischio di similari violazioni in futuro	