Città di **Vicenza**

Insignita di due Medaglie d'Oro al Valore Militare
per il Risorgimento e la Resistenza

PROTOCOLLO DATA BREACH

Protocollo per la rilevazione, valutazione e gestione delle violazioni di dati personali ai sensi degli articoli 33 e seguenti Regolamento UE 679/2016 (Regolamento generale sulla protezione dei dati)

Versione	Attività	Data
01	Creazione	15.01.2024

Sommario

1. Premessa e ambito di applicazione

Il 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 - di seguito anche solo "GDPR") definisce la **violazione dei dati personali**, o "***data breach***", come la "**violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati".**

La violazione di dati personali può configurarsi con molteplici modalità, quali, ad esempio, un attacco informatico, accessi abusivi, incidenti, fenomeni naturali (es. incendio), perdita o furto di un supporto informatico, perdita di documenti cartacei o consultazioni da parte di soggetti non autorizzati.

Si tratta di eventi che, se non affrontati in modo adeguato e tempestivo, possono provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione ai 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 (vd. Considerando 85 GDPR).

Al fine di garantire la sicurezza e riservatezza dei dati personali, anche nel rispetto del principio di "accountability", con il presente protocollo (di seguito il "Protocollo") il Comune di Vicenza, quale titolare del trattamento, intende fornire alcune informazioni sul concetto di violazione dei dati personali nonché individuare le procedure da seguire in caso di avvenuta violazione ai fini della rilevazione della violazione, nonché le indicazioni per valutarne i rischi, contenerne gli effetti negativi e porvi rimedio.

2. Normativa di riferimento

Il presente Protocollo si basa sulle seguenti fonti:

- "*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*" - GDPR;
- "*Reccomandations for a methodology of the assessment of severity of personal data breaches*"- December 2013 – European Union Agency for Network and Information Security ("Enisa");
- parere 03/2014 WP 2013 del 25 marzo 2014 "Parere sulla notifica delle violazioni di dati personali";
- linee guida del WP29 ("Article 29 Data Protection Working Party") del 03.10.2017 "*Guidelines on Personal data breach notification under Regulation 2016/679" (revisione del 06.02.2018);*
- linee guida del WP29 ("Article 29 Data Protection Working Party" del 04.10.2017 "*Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*";
- "*Guidelines 01/2021 on examples regarding data breach notifications*" adopted on 14 December 2021 – version 2.0 adopted after public consultation - European Data Protection Board.

3. Definizioni generali

Nel presente Protocollo sono adottate le seguenti definizioni:

Il Comune o l'Ente: il Comune di Vicenza;

Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile. 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 on line o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

Dati particolari: dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, dati genetici, dati biometrici intesi ad identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale (art. 9 GDPR);

Interessato: la persona fisica identificata o identificabile a cui si riferisce il dato trattato;

Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

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;

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 ai sensi dell'art. 28 GDPR;

Garante: Garante per la protezione dei dati personali;

DPO: Responsabile della protezione dei dati;

SIC: Settore Informatico Comunale.

4. Ambito di applicazione e destinatari

La procedura prevista dal presente Protocollo è obbligatoria per tutti i **dipendenti** e gli **amministratori** del Comune, nonché dei **consulenti/collaboratori** che eseguono operazioni di trattamento dati di cui il Comune è titolare del trattamento nell'ambito delle proprie mansioni lavorative o contrattuali.

Il Protocollo integra le istruzioni impartite nelle nomine a designati e autorizzati al trattamento e si applica a tutte le violazioni di sicurezza che possono verificarsi nelle attività di trattamento dati svolte nel Comune, sia con strumenti informatici che in modalità analogica.

Il mancato rispetto della procedura indicata nel presente Protocollo può costituire fonte di responsabilità disciplinare da parte del personale dipendente del Comune in conformità alla normativa e al Contratto Collettivo Nazionale del Lavoro vigente e, per i collaboratori/consulenti/responsabili del trattamento, fonte di responsabilità contrattuale, fatto salvo in ogni caso il diritto al risarcimento dei danni subiti dall'Ente nei confronti del responsabile.

Si rappresenta comunque che le segnalazioni possono provenire anche da terzi (es. dagli interessati).

5. Definizione di data breach

Come anticipato nelle premesse, la violazione dei dati personali, o "*data breach*", è definita all'art. 4 GDPR come la "**violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati".**

Le violazioni possono essere suddivise nelle seguenti categorie:

a. **Violazioni di riservatezza**: nel caso in cui si verifichi una **divulgazione** o un **accesso** a dati personali non autorizzato od accidentale;
b. **Violazioni di integrità**: nel caso in cui si verifichi una **modifica** dei dati non autorizzata od accidentale;
c. **Violazioni di disponibilità**: nel caso in cui si verifichi una non autorizzata od accidentale **perdita** o **distruzione** dei dati. La "perdita di dati" si ha quanto i dati, presumibilmente, esistono ancora ma il titolare ne ha perso il controllo oppure la possibilità di accedervi. La "distruzione" dei dati si ha quando i dati non esistono più oppure, pur esistendo, non hanno più un formato utilizzabile dal titolare.

La violazione dei dati, a seconda delle circostanze, può rientrare in uno solo dei casi di cui sopra, o in tutti e tre.

Al fine di comprendere meglio le possibili casistiche di *data breach*, si riportano di seguito ulteriori esempi chiarificatori.

ESEMPI DI POSSIBILI DATA BREACH

1. Attacco ransomware con criptazione dei dati;
2. furto o smarrimento di tablet/notebook/smartphone di proprietà dell'Ente;
3. invio di e-mail contenente dati personali a un destinatario errato;
4. furto o perdita di fascicoli/documentazione cartacei o loro distruzione ad esempio in seguito a incendio/ allegamento di un archivio cartaceo;
5. dati cancellati accidentalmente o da una persona non autorizzata;
6. accesso abusivo al sistema informatico da parte di soggetti non autorizzati, con o senza successiva rivelazione dei dati a terzi;
7. interruzione significativa di un servizio pubblico che renda i dati indisponibili, anche per un periodo di tempo limitato;
8. violazione di misure di sicurezza fisiche (es. accesso illegittimo ad archivi contenenti dati personali)
9. perdita della chiave di decifratura di dati personali crittografati;
10. pubblicazione sul sito istituzionale di dati personali che non dovevano essere pubblicati.

6. Rilevazione interna del data breach

Chiunque operi all'interno dell'organizzazione del Comune, qualora rilevi un'eventuale violazione di dati personali, **deve contattare immediatamente il SIC,** all'indirizzo sistemi_informativi@comune.vicenza.it utilizzando il modello di segnalazione "Modello interno di segnalazione di un data breach" (Allegato A).

Qualora la segnalazione avvenga senza l'utilizzo del predetto modulo, il SIC, non appena ricevuta la segnalazione, invierà al segnalante il modello chiedendone la compilazione e immediata restituzione, al fine di ottenere quanto prima tutte le informazioni necessarie per valutare l'evento.

ATTENZIONE

La violazione dei dati non deve essere celata, in quanto l'oscuramento della notizia, oltre a esporre il titolare del trattamento a gravi sanzioni amministrative pecuniarie, amplifica in modo sensibile gli effetti negativi dell'evento e può ostacolare la tutela dell'interessato.

7. Rilevazione del data breach da parte dei responsabili del trattamento

L'obbligo di informazione grava anche sui responsabili del trattamento nominati dall'Ente, i quali devono informare l'Ente entro la tempistica indicata nella nomina inviando una PEC all'indirizzo del Comune vicenza@cert.comune.vicenza.it indicando come oggetto "**all'attenzione del SIC - segnalazione data breach**" in modo da permettere al Comune di rispettare i termini per gli adempimenti di cui all'art. 33 GDPR. Il responsabile deve comunicare all'Ente qualsiasi violazione dei dati personali, a prescindere dai possibili rischi derivanti dalla violazione. Il SIC dovrà chiedere al responsabile del trattamento tutte le informazioni necessarie per la gestione dell'evento, chiedendo eventualmente la compilazione dell'Allegato A.

8. Primi adempimenti e valutazione preliminare

Una volta ricevuta la notizia di un potenziale data breach, il SIC avviserà immediatamente il DPO, inoltrando la segnalazione ricevuta, e si riunirà, entro 24 ore dalla comunicazione dell'incidente, salvo eccezionali comprovati e documentati motivi, per effettuare una valutazione preliminare volta a valutare la natura dell'evento.

In particolare si provvederà a:

- identificare il dispositivo interessato (es. computer, apparato di rete, sistema di back up, ecc.), la causa dell'evento (inclusa la natura colposa o dolosa), se siano coinvolti o meno dati personali e la loro natura;
- identificare le categorie di interessati coinvolti (es. dipendenti, cittadini, ecc.);

- verificare se permanga o meno la disponibilità del dato;
- individuare le eventuali misure per trattare i rischi.

Qualora si sia verificato un effettivo caso di *data breach*, il SIC procederà con gli adempimenti indicati nei paragrafi successivi (valutazione del rischio, annotazione nel registro delle violazioni, misure correttive).

Si rappresenta che se dall'analisi preliminare risulti che l'evento non sia un effettivo data breach, lo stesso dovrà comunque essere annotato nel registro delle violazioni (*vd. infra*).

9. Valutazione del rischio connesso al data breach

Il livello di rischio che una violazione dei dati personali può presentare per i diritti e le libertà delle persone fisiche è definito sulla base dei seguenti due parametri:

- **PROBABILITA'**, ovvero il grado di possibilità che la violazione segnalata presenti un rischio;
- **GRAVITA'**, ovvero la rilevanza degli effetti pregiudizievoli che la violazione è in grado di produrre.

Ai fini della valutazione della gravità della violazione, il Comune ha ritenuto di avvalersi della metodologia proposta e progettata dall'ENISA nelle "*Reccomandations for a methodology of the assessment of severity of personal data breaches*" di dicembre 2013, a cui si effettua espresso rinvio.

Secondo la metodologia ENISA, i criteri principali che devono essere tenuti in considerazione per valutare la gravità di un caso di *data breach* **("Severity of data breach" o "SE")** sono:

- **contesto del trattamento dei dati ("Data Processing Context" o"DPC")**: individua il tipo di violazione di dati, unitamente ad ulteriori fattori correlati al contesto complessivo del trattamento. Il contesto costituisce l'elemento principale della valutazione;
- **facilità di identificazione dell'individuo a cui appartengono i dati violati ("Ease of Identification" o "EI")**: stabilisce la facilità con la quale si può risalire all'identità degli interessati sulla base della tipologia di dati coinvolti nella violazione. Questo criterio costituisce un fattore correttivo del DCP;
- **circostanze della violazione ("Circumstances of breach" o "CB")**: indirizza le circostanze specifiche della violazione, correlate al tipo di violazione, includendo la perdita di sicurezza e gli intenti malevoli. Quantificano specifiche circostanze della violazione, che possono esserci o meno. Quando sono presenti, possono solo aumentare la gravità della violazione.

ENISA suggerisce quindi di assegnare un punteggio ai vari criteri, la combinazione dei quali permette di valutare la gravità della violazione, la quale è data dalla formula seguente:

SE= (DPC x EI) + CB

dove

SE = gravità della violazione
EI= facilità di identificazione
DPC= contesto della violazione
CB= circostanze della violazione

Il risultato sarà dato da un valore che rientrerà nei quattro livelli di gravità: bassa, media, alta e molto alta, di seguito riportati:

Gravità della violazione	Rischio	Descrizione
SE < 2	Basso	Gli interessati non incontreranno inconvenienti o potrebbero incontrare alcuni inconvenienti, che supereranno senza alcun problema (tempo passato a reinserire le informazioni, fastidio, irritazione, ecc…)
2≤ SE < 3	Medio	Gli interessati possono incontrare inconvenienti significativi, che saranno in grado di superare nonostante alcune difficoltà (costi extra, diniego di accesso ai servizi aziendali, paura, mancanza di comprensione, stress, disturbi fisici lievi, ecc…)
3 ≤ SE <4	Alto	Gli interessati possono incontrare conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, lista nera da parte delle banche, danni alla proprietà, perdita del posto di lavoro, citazioni a giudizio, peggioramento della salute, ecc…)
4 ≤ SE	Molto alto	Gli interessati possono incontrare significativi, o anche irreversibili, conseguenze, che non possono superare (difficoltà finanziarie come debito sostanziale, inabilità al lavoro, disturbi psicologici a lungo termine o disturbi fisici, morte, ecc…)

(*Tabella 01)*

Il SIC, con il supporto del DPO, provvederà ad effettuare nel più breve tempo possibile la valutazione della gravità dell'evento, e a condividerla con il Sindaco, documentandola in modo adeguato, in modo che il Comune possa procedere con l'eventuale notifica al Garante e comunicazione agli interessati, ove ve ne siano i presupposti.

Sebbene i criteri e le esemplificazioni elaborate da ENISA siano certamente utili ai fini della valutazione del rischio, la valutazione deve essere effettuata sulla base delle circostanze del caso concreto.

10. Risoluzione dell'incidente di sicurezza

Il SIC, con il supporto del DPO, dei propri fornitori di servizi IT e di eventuali ulteriori consulenti procederà all'adozione di tutte le misure necessarie per il Comune per fronteggiare l'incidente e mitigarne i rischi. A titolo esemplificativo e non esaustivo, le azioni comprendono:

- individuazione dei dati, sistemi e dispositivi compromessi;
- gestione o attenuazione della causa della violazione;
- localizzazione e reperimento dei *log* e di tutte le prove informatiche necessarie per eventuali prove legali, raccolte e conservate con le opportune tecniche della *digital forensics,* anche con l'ausilio di consulenti esterni;
- nel caso di sospettata attività criminale correlata alla violazione, comunicazione al Sindaco per l'adozione delle azioni più opportune (es. denuncia alle Autorità competenti, azioni legali, ecc.).

Potranno essere adottate eventuali misure ulteriori, a seconda del tipo di violazione occorsa.

A seguito del *data breach* si procederà alla revisione delle misure di sicurezza in atto, delle policy e procedure aziendali, al fine di migliorare e prevenire eventuali ulteriori incidenti.

11. Notifica al Garante

Ai sensi dell'art. 33 GDPR, la notifica al Garante è obbligatoria a meno che sia improbabile che la violazione presenti rischi per i diritti e le libertà delle persone fisiche.

La notifica è quindi obbligatoria qualora la gravità della violazione sia di un **livello superiore a quello "Basso**" (vd. Tabella 01).

Qualora si debba effettuare la notifica, il SIC, **entro 48 ore dalla segnalazione,** salvo motivate situazioni eccezionali, procederà alla raccolta e rielaborazione delle informazioni e documentazione relativa al *breach* necessarie al fine della notifica, quali:

- data e ora in cui la violazione si è verificata;
- data e ora in cui si è appresa la violazione;
- natura e causa della violazione;
- descrizione della violazione;
- categorie di interessati coinvolti e numero approssimativo;
- tipologie di dati personali oggetto di violazione;
- misure di sicurezza in essere al momento della violazione;
- modalità con cui si è appresa la violazione;
- ulteriori soggetti connessi al trattamento;
- probabili conseguenze della violazione;
- misure adottate a seguito della violazione;
- valutazione del rischio per gli interessati;
- comunicazione agli interessati;
- informazioni relative a violazioni transfrontaliere.

Entro 72 ore dalla segnalazione il Sindaco o suo delegato, con il supporto del DPO, procede alla notifica **mediante la procedura presente sul sito del Garante, indicando tutte le informazioni richieste**.

In base all'attuale procedura del Garante, la notifica può essere di tre tipi:

i. **prima notifica** "**completa**": da effettuarsi qualora si disponga già di tutte le informazioni richieste, siano state effettuate tutte le valutazioni necessarie anche con il DPO e si voglia portare a termine il completamento del processo di notifica;

ii. **prima notifica "preliminare**": da effettuarsi, sempre entro la tempistica, qualora non si disponga di tutte le informazioni necessarie. In questo caso si è sempre tenuti ad effettuare una successiva notifica integrativa con la quale si comunica il completamento del processo di notifica, indipendentemente dal fatto che vengano fornite o meno ulteriori informazioni sulla violazione;

iii. **notifica "integrativa**": questa notifica può essere utilizzata sia per fornire le informazioni necessarie assenti nelle precedenti notifiche, sia per comunicare il completamento del processo di notifica, che per fornire informazioni aggiuntive di cui il Comune è venuto a conoscenza nel tempo. Per la trasmissione di una notifica integrativa è necessario far riferimento al numero di fascicolo, e al relativo PIN, che la procedura assegna successivamente alla trasmissione della prima notifica. La notifica integrativa può essere utilizzata anche per annullare una precedente notifica, qualora una successiva indagine dimostri che l'incidente di sicurezza è stato contenuto e che non si è verificata alcuna violazione.

La scelta di procedere alla notifica "completa" o "preliminare" dovrà essere opportunatamente documentata.

Si raccomanda di consultare la pagina dedicata sul sito del Garante per verificare eventuali aggiornamenti alla procedura di notifica.

E' possibile effettuare la notifica anche dopo le 72 ore (c.d. "**notifica tardiva**"), purché la notifica sia corredata dalle ragioni del ritardo.

Si ricorda che **il termine di 72 decorre dal momento in cui il titolare ha avuto conoscenza della violazione dei dati**, ovvero quando il titolare ha avuto un **ragionevole livello di certezza** circa l'avvenimento di un incidente alla sicurezza che ha determinato la compromissione di dati personali.

La consapevolezza della violazione dei dati personali può dipendere molto dalle circostanze, perché alcune violazioni possono essere facilmente individuabili, altre invece possono richiedere un'indagine più approfondita. Durante le indagini, il titolare può essere considerato come privo di un grado di conoscenza tale da far scattare immediatamente l'obbligo di notifica. Si precisa comunque che la fase investigativa non deve essere abusata per prorogare illegittimamente il termine di notifica.

La documentazione inerente alla notifica dovrà essere conservata dal SIC.

12. Casi in cui non è obbligatoria la notifica al Garante.

L'art. 33, paragrafo 1, GDPR, precisa che **la notifica non è necessaria se è improbabile che la violazione dei dati presenti un rischio per i diritti e le libertà delle persone fisiche.**

Il titolare è tenuto quindi ad effettuare un'attenta analisi sugli effetti che la violazione può comportare sui diritti degli interessati, al fine di decidere se procedere o meno alla notifica al Garante. In caso di dubbio, è opportuno mantenere un atteggiamento di prudenza ed effettuare la notifica.

L'evento dovrà essere comunque annotato nel registro delle violazioni, unitamente alle motivazioni alla base della decisione della omessa notifica (*vd. infra*).

13. Comunicazione della violazione dei dati personali all'interessato (art. 34 GDPR)

L'art. 34 GDPR stabilisce l'obbligo di effettuare la comunicazione della violazione agli interessati nel caso in cui la violazione sia suscettibile di presentare **un rischio elevato** per i diritti e le libertà delle persone fisiche. Di conseguenza, qualora sulla base della valutazione del rischio di cui alla Tabella 01 emerga che la violazione di dati personali comporti un rischio elevato per gli interessati (livello "**Alto**" o "**Molto Alto**"), il Comune procederà a comunicare la violazione all'interessato, senza ingiustificato ritardo.

La comunicazione all'interessato di cui al paragrafo 1 dell'art. 34 GDPR deve descrivere con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contenere almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d), GDPR, ovvero:

- la descrizione della natura della violazione;
- il nome e i contatti del DPO;
- una descrizione delle possibili conseguenze della violazione;
- una descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati e anche, se del caso, per attenuarne i possibili effetti negativi. È opportuno che il titolare suggerisca agli interessati i possibili accorgimenti per proteggersi dagli effetti della violazione, come, ad esempio, modificare le password.

Il Sindaco provvederà a valutare, di concerto con il SIC il Settore Comunicazione, Informazione, Portale della Città e il DPO, le modalità più opportune di comunicazione, privilegiando modalità dirette con gli interessati, quali ad esempio e-mail o comunicazioni scritte individuali, salvo che ciò non richieda uno sforzo sproporzionato. In tal caso è possibile procedere con una comunicazione pubblica (es. pubblicazione sul sito internet istituzionale – vd. *infra*).

Si riporta a titolo esemplificativo un facsimile di comunicazione, che potrà essere utilizzato compatibilmente con la forma scelta (**Allegato B)**.

Non è richiesta la comunicazione all'interessato qualora ricorra uno dei casi previsti dal paragrafo 3 dell'art. 34 GDPR, quali:

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 all'art. 34, par. 1, GDPR;
c. la 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.

14. Registro delle violazioni (art. 33, paragrafo 5, GDPR)

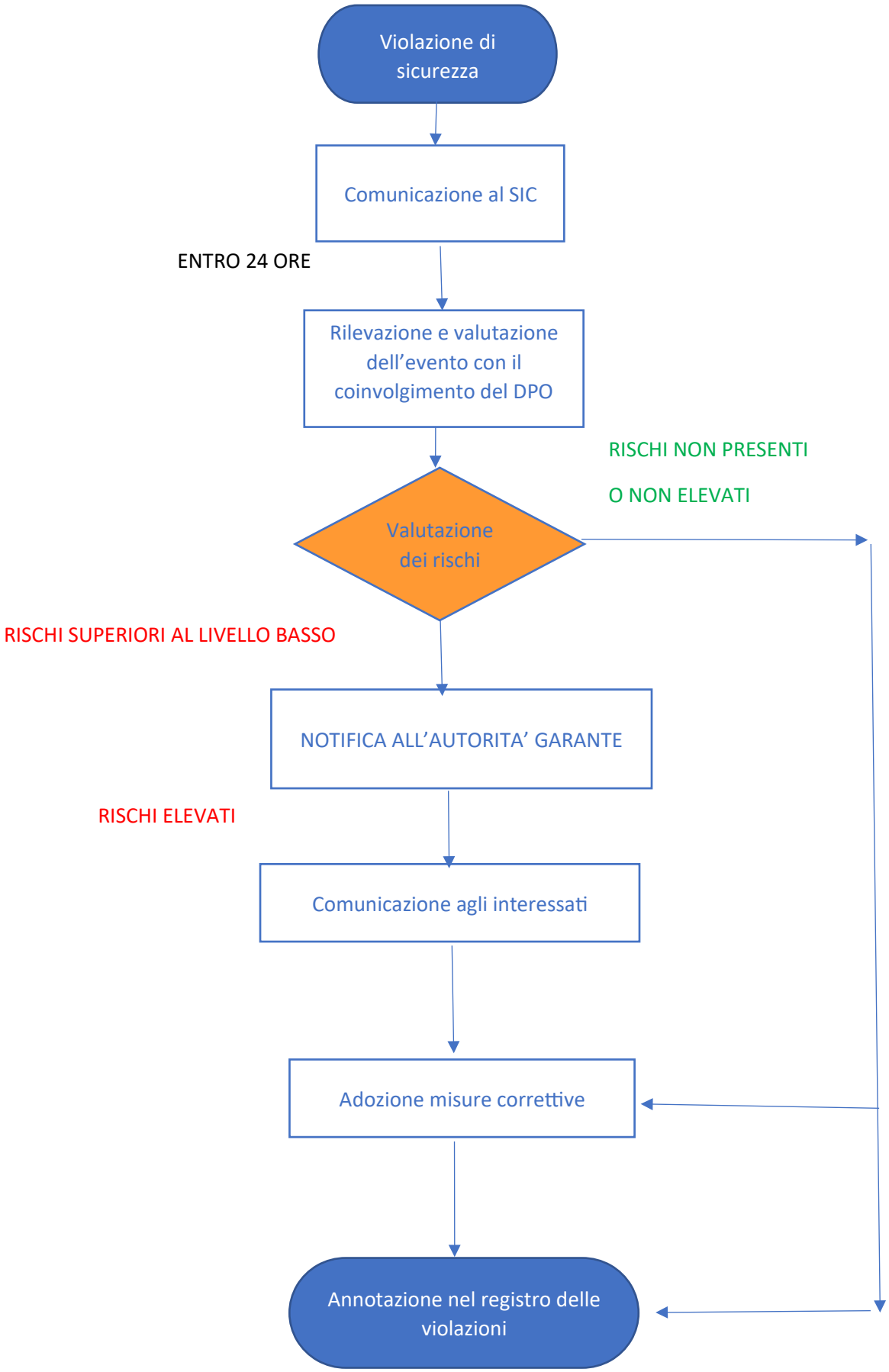
Una volta ricevuta la segnalazione di un *data breach*, il SIC con il supporto del DPO provvederà ad annotarla nel "Registro delle violazioni", a prescindere dalla notifica al Garante, sulla base del modello allegato al presente Protocollo (**Allegato C**). Il registro deve indicare in particolare:

- le circostanze relative alla violazione;
- le conseguenze;
- i provvedimenti adottati per porvi rimedio.

Nel registro devono essere annotate tutte le decisioni adottate dal Comune in occasione del *data breach*, inclusa la decisione di non effettuare la notifica al Garante, o in caso di notifica tardiva, i motivi del ritardo.

Il SIC provvede alla conservazione del Registro delle violazioni e di tutta la documentazione inerente alla violazione, compresa quella relativa ai provvedimenti adottati per porre rimedio alle violazioni, a disposizione del Garante in caso di eventuali controlli.

FLUSSO DI GESTIONE DEI DATA BREAC



Allegato A – Modello interno di segnalazione di un data breach

Settore Informatico Comunale (SIC)
sistemi_informativi@comune.vicenza.it

Dati del segnalante	
Nome e cognome	
Area/Settore/Ufficio di appartenenza	
Indirizzo e-mail	
Numero di telefono	

Descrizione evento	
Descrizione dell'incidente (cosa è successo)	
Data e ora dell'incidente	
Cause dell'incidente (perché è successo)	
Sistemi, banche dati, supporti interessati	
Come è stato rilevato l'incidente? Quando?	
Area/Settore coinvolto	
Ulteriori indicazioni utili	
Eventuali allegati	

Luogo e data, _____

Firma

_____

Allegato B – Modello comunicazione di una violazione di dati personali agli interessati ai sensi dell'art. 34 del Regolamento UE 679/2016

Gentile Signora, Egregio Signore,

con la presente Le comunichiamo che purtroppo si è verificata una violazione dei nostri sistemi informatici che ha riguardato anche i Suoi dati personali (*oppure*) che si è verificato...

La violazione è stata prontamente affrontata dai nostri esperti di sicurezza informatica e dal Responsabile per la protezione dei dati per ridurre ulteriormente l'esposizione dei Suoi dati personali e le possibili conseguenze della violazione. Ci stiamo adoperando per fare tutto quanto è in nostro potere per garantire che il danno sia mitigato e che ciò non accada di nuovo in futuro.

È nostro obbligo fornirLe in modo chiaro e semplice tutte le informazioni relative alla violazione, in modo da arginare il più possibile le conseguenze della violazione stessa.

Cosa è accaduto
descrivere la violazione, precisando la cronologia degli eventi, senza indicare informazioni sensibili sull'Ente, a meno che non sia indispensabile per descrivere la violazione

Dati personali coinvolti
Elencare i tipi di dati personali.

Conseguenze della violazione
Descrivere le probabili conseguenze della violazione, tenuto conto della natura della violazione e dei tipi di dati personali coinvolti.

Misure adottate e proposte al fine di attenuare i possibili effetti negativi
Per porre rimedio alla violazione e per attenuare i possibili effetti negativi abbiamo adottato le seguenti misure:

Le suggeriamo di …… (elencare le azioni che l'interessato dovrà approntare)

Come eviteremo in futuro tale problematica
Al fine di evitare che tale violazione si verifichi nuovamente e di ridurre al minimo l'impatto sugli interessati abbiamo attivato le seguenti azioni:
elencare le azioni intraprese dal Comune per garantire che questa violazione non venga ripetuta, senza compromettere la riservatezza dell'organizzazione, rassicurando nel contempo l'interessato.

E' stata effettuata la notifica al Garante per la protezione dei dati personali ai sensi dell'art. 33 Regolamento UE 679/2016.

Per ulteriori informazioni si prega di contattare il ---- o il Responsabile per la protezione dei dati personali all'indirizzo dpo@comune.vicenza.it.

lì,

Il Comune di Vicenza

Allegato C – Registro delle violazioni

REGISTRO DELLE VIOLAZIONI - COMUNE DI VICENZA											
N° violazione	Data e ora della violazione	N° interessati coinvolti	Tipologia di dati personali coinvolti	Origine violazione	Descrizione della violazione	Come siamo venuti a conoscenza della violazione	Conseguenza della violazione	Azioni correttive intraprese	Comunicazione al Garante	Comunicazione agli interessati	Data di chiusura della violazione