PROCEDURA
DI GESTIONE DELLA VIOLAZIONE DI DATI
(*DATA BREACH*)

Regolamento (UE) 2016/679
Regolamento generale sulla protezione dei dati.

(approvato con delibera di Giunta n.126 del 07/12/2022)

Scheda descrittiva

Anagrafica del documento

Titolo	**:**	Procedura di gestione della violazione di dati (*data breach*)
Tipo documento	**:**	Procedura
Descrizione	**:**	Il documento descrive le modalità operative da seguire in caso di violazione dei dati personali avvenuta sia a seguito di trattamento informatizzato sia a seguito di trattamento cartaceo.

INDICE

1 PREMESSA

Il 25 maggio 2018 è diventato definitivamente applicabile in tutti i Paesi europei il Regolamento generale sulla protezione dei dati 2016/679 (di seguito "GDPR") con ricadute organizzative, operative e tecnologiche che riguardano i principali processi di gestione dei dati personali. Tra le novità contenute nel Regolamento, anche alcuni oneri aggiuntivi per la gestione degli incidenti di sicurezza che comportano la violazione di dati personali (*data breach*).

2 CONTESTO DI RIFERIMENTO E QUADRO GIURIDICO

Le norme di riferimento sono:

1. Regolamento UE n. 679/2016 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);
2. Documento WP 250 "Guidelines on Personal data breach notification under Regulation 2016/679" del 3 ottobre 2017;
3. Linee guida 01/2021 sugli esempi riguardanti la notifica di violazione dei dati.

3 FINALITA'

La finalità di questa procedura organizzativa interna è quella di fornire delle indicazioni pratiche ed operative, individuando la metodologia che consenta la gestione delle violazioni dei dati personali trattati dal Comune di Breda di Piave in qualità di Titolare del trattamento.

4 CATEGORIE DEI DATI OGGETTO DELLA PROCEDURA DI SEGNALAZIONE DEL DATA BREACH

I dati oggetto di riferimento sono i dati personali trattati "da" e "per conto" del Titolare del trattamento, in qualsiasi formato (inclusi documenti cartacei) e con qualsiasi mezzo.

In particolare, essi si distinguono nelle seguenti categorie:

- **dati "comuni" che permettono l'identificazione diretta** – come i dati anagrafici (ad esempio nome e cognome), le immagini, ecc. – e **l'identificazione indiretta,** come un numero di identificazione (ad esempio, il codice fiscale, l'indirizzo IP, il numero di targa);

- **dati rientranti in categorie particolari:** si tratta dei "*dati che rilevino l'origine razziale od etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale di una persona*" (art. 9 GDPR);

- **dati relativi a condanne penali e reati:** si tratta dei dati c.d. "*giudiziari*", cioè quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato. Il Regolamento (UE) 2016/679 (art. 10 GDPR) ricomprende in tale nozione i dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza.

Per maggior dettaglio si rinvia alla tabella presente in Appendice 2.

5 CRITERI PER INDIVIDUARE E CLASSIFICARE UN *DATA BREACH*

Un *data breach*, o violazione di dati personali, è un incidente 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"*.

In relazione ad un evento che si è verificato o che si presume si possa verificare (minaccia) come conseguenza di un altro evento illecito o accidentale, la violazione di dati personali viene classificata in tre tipologie:

Tipologia di violazione	Evento/Minaccia	Esempi
Violazione di riservatezza	Accesso o trattamento non autorizzato o illecito	Quando nella redazione di un atto non si redige la versione con omissione dei dati da non pubblicare e l'atto viene pubblicato nella sua interezza; quando si inoltrano messaggi contenenti dati a soggetti non interessati al trattamento.
	Divulgazione non autorizzata	
Violazione di integrità	Modifica non autorizzata o accidentale	I dati potrebbero essere danneggiati o non più completi nel momento di un aggiornamento delle informazioni
Violazione di disponibilità	Perdita o distruzione accidentale o illegale	La perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità
	Indisponibilità temporanea o prolungata	

Tabella 1 – Classificazione di un data breach

Le tipologie non sono mutuamente esclusive: una violazione di dati personali può riguardare contemporaneamente la riservatezza, l'integrità e la disponibilità, una di esse o una loro combinazione.

6 PRINCIPALI RISCHI CONNESSI AL DATA BREACH

La violazione dei dati può comportare elevati rischi per i diritti e le libertà delle persone fisiche.
I rischi principali sono:

- danni fisici, materiali o immateriali alle persone fisiche;
- perdita del controllo dei dati personali;
- limitazione dei diritti, discriminazione;
- furto d'identità;
- perdite finanziarie, danno economico o sociale.

7 DESTINATARI DELLA PROCEDURA DI GESTIONE DEL *DATA BREACH*

La presente procedura interna è obbligatoria per tutti:

- gli AUTORIZZATI al trattamento: lavoratori dipendenti e terzi non dipendenti che hanno accesso ai dati personali trattati nel corso della propria attività lavorativa presso il Comune di Breda di Piave;
- i RESPONSABILI ESTERNI ex art. 28 GDPR che, in ragione del rapporto contrattuale in essere con il Titolare, trattano dati per conto dello stesso.

La mancata conformità alle regole di comportamento previste dalla stessa può comportare provvedimenti disciplinari a carico dei dipendenti inadempienti, ovvero la risoluzione dei contratti in essere con terze parti inadempienti, secondo le normative vigenti in materia.

8 COMPITI DEL TITOLARE DEL TRATTAMENTO PER PREVENIRE FENOMENO *DATA BREACH*

Tale procedura si applica, tenendo conto delle rispettive specificità, sia a trattamenti informatizzati sia a trattamenti eseguiti senza l'ausilio di strumenti informatici.

Per trattamenti informatizzati nell'ambito di questo documento si intendono quelli effettuati mediante applicazioni o strumenti di office automation. In tale ambito si fa riferimento alle misure tecniche ed organizzative adottate per la riduzione del rischio residuo come descritte nel Registro dei Trattamenti.

Per trattamenti non informatizzati nell'ambito di questo documento si intendono quelli effettuati senza l'ausilio di strumenti elettronici, ovvero nei casi in cui i dati risiedono su supporto cartaceo. In tale ambito assumono significativa rilevanza le istruzioni impartite per iscritto, sia al momento della nomina sia mediante apposite policies aziendali, alle persone autorizzate (c.d. Autorizzati al trattamento) finalizzate all'utilizzo, al controllo e alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali, in special modo se contenenti dati personali sensibili, ipersensibili e giudiziari, e l'adozione degli adeguati comportamenti da parte degli autorizzati stessi.

In particolare il Titolare:

- individua, e verifica periodicamente, gli incaricati del trattamento che utilizzano strumenti non automatizzati per la raccolta e la gestione di dati personali e impartisce loro istruzioni scritte relative alla gestione dei dati e alla loro custodia;

- identifica e comunica agli incaricati gli archivi in cui riporre i documenti contenenti i dati personali e/o categorie particolari di dati (armadi chiusi a chiave, stanze chiuse a chiave, casseforti di sicurezza, ecc.);

- istruisce le persone autorizzate affinché i documenti cartacei vengano conservati in archivi adeguatamente protetti per evitare la lettura e/o il prelievo non autorizzato, garantendo, quindi, la riservatezza e l'integrità dei dati personali in essi contenuti;

- dispone che i documenti cartacei vengano custoditi in appositi archivi chiusi a chiave, in armadi o stanze, al termine della giornata lavorativa; le chiavi devono essere risposte in un luogo sicuro e non lasciate nelle serrature stesse;

- prevede, ove possibile, la conservazione dei documenti contenenti dati personali di categorie particolari (ad esempio sensibili e/o giudiziari) separata dai documenti contenenti dati personali comuni;

➢ dispone che il trattamento di dati personali e/o di categorie particolari degli stessi avvenga nel rispetto del principio di limitazione della finalità, ovvero unicamente per lo scopo per cui sono stati raccolti;

➢ istruisce le persone autorizzate affinché:
- i dati personali e/o le categorie particolari degli stessi non vengano diffusi o comunicati a soggetti non autorizzati al trattamento;
- non vengano lasciati incustoditi documenti contenenti i dati personali e/o le categorie particolari degli stessi durante e dopo l'orario di lavoro;
- non vengano lasciati in luoghi accessibili al pubblico i documenti contenenti i dati personali e/o le categorie particolari degli stessi;
- i documenti vengano riposti negli archivi quando non più operativamente necessari;
- limitino allo stretto necessario l'effettuazione di copie dei suddetti documenti;
- verifichino la corretta esecuzione delle procedure di distruzione dei documenti, quando non più necessari o quando richiesto dall'interessato, attraverso l'utilizzo di opportuni strumenti (distruggi documenti), in modo da rendere impossibile la ricostruzione del documento.

9 PROCESSO DI NOTIFICA DI PRESUNTO *DATA BREACH*

Nel caso in cui, nonostante le misure adottate dal Titolare, si verifichino uno o più eventi di cui alla tabella 1, il flusso operativo che viene seguito è qui sotto illustrato.

9.1 ACQUISIZIONE DEL DATA BREACH (RILEVAZIONE EVENTO, INVIO SEGNALAZIONE, RACCOLTA INFORMAZIONI E COMUNICAZIONE *DATA BREACH*).

- Ogni autorizzato al trattamento deve avvisare immediatamente l'assistenza tecnica o il Data Protection Officer-Responsabile della protezione dei dati (di seguito "DPO") dell'Ente, segnalando le violazioni o gli incidenti informatici che ha rilevato e che possono avere impatto significativo sui dati personali, con la più ampia libertà di forme e procedure (anche per le vie brevi e/o oralmente);
- dovrà seguire nel più breve tempo possibile formale comunicazione completa dei dettagli sull'evento segnalato con mail all'indirizzo del DPO reperibile sul sito istituzionale del Comune di Breda di Piave in Amministrazione Trasparente nella sezione "*Altri Contenuti –Privacy*"; per tale comunicazione potrà essere utilizzato l'allegato **Modulo di comunicazione data breach (Allegato A)** (si ricorda che il GDPR fissa in 72 ore il tempo massimo che deve intercorrere dal momento in cui si è venuto a conoscenza della violazione e la notifica al garante se del caso);

9.2 GESTIONE TECNICA (ACCERTAMENTO, RACCOLTA INFORMAZIONI, DEFINIZIONE SOGGETTI COINVOLTI, EVENTUALI AZIONI CORRETTIVE).

- Ai fini del rispetto dei tempi prescritti dalla normativa, d'intesa con il Titolare del trattamento, il DPO provvederà immediatamente e comunque non oltre le 24 ore successive alla ricezione della comunicazione a convocare una sorta di "tavolo tecnico", che in base alla tipologia di segnalazione ricevuta, vedrà la partecipazione del personale del Comune per effettuare la valutazione preliminare sulla probabilità e gravità dei rischi per i diritti e le libertà degli interessati che possono derivare da trattamenti dei dati personali oggetto di violazione;
- il Titolare, unitamente al DPO, avvia tempestivamente in particolar modo azioni correttive necessarie per gestire tecnicamente la violazione e per ripristinare, se del caso, la disponibilità e l'accesso dei dati personali (ad es. riparazione fisica di strumentazione; utilizzo dei file di back up per recuperare dati persi o danneggiati; isolamento/chiusura di un settore compromesso della rete; cambio dei codici di accesso… ecc.);
- il DPO dovrà quindi curare e documentare l'attività istruttoria, acquisendo tutti gli elementi probatori necessari per una adeguata valutazione;
- all'esito delle attività dovrà essere raccolta da parte del DPO la documentazione di supporto, ricognitiva delle analisi e degli esiti della valutazione effettuata nonché delle conseguenti proposte operative, da sottoporre al Titolare del trattamento per la decisione finale.

9.3 VALUTAZIONE DI IMPATTO

- Il Titolare effettua una valutazione di impatto dell'evento verificatosi, consultandosi con il DPO ed avvalendosi, se nel caso, di eventuali altre professionalità necessarie per la corretta analisi della situazione.

In particolare:

A) identifica la violazione ed individua a quale categoria può appartenere:

• **di riservatezza**, quando si verifica una divulgazione o un accesso ai dati non autorizzato o accidentale;

• **di integrità**, quando si verifica un'alterazione di dati personali non autorizzata o accidentale;

• **di disponibilità**, quando si verifica perdita, inaccessibilità, o istruzione, accidentale o non autorizzata;

B) valuta il rischio connesso alla violazione.

Il livello di rischio è definito sulla base di due parametri, gravità e probabilità:

GRAVITA' rilevanza degli effetti pregiudizievoli che la violazione è in grado di produrre sui diritti e le libertà delle persone coinvolte	Impatto della violazione sui diritti e le libertà delle persone coinvolte: • basso: nessun impatto • medio: impatto poco significativo, reversibile • alto: impatto significativo, irreversibile
PROBABILITA' grado di possibilità che si verifichino uno o più eventi temuti (es. la perdita di ogni traccia dei dati).	Possibilità che si verifichino uno o più eventi temuti • basso: l'evento temuto non si manifesta • medio: l'evento temuto potrebbe manifestarsi • alto: l'evento temuto si è manifestato

Ai fini della identificazione dei valori da attribuire ai due parametri per la valutazione del rischio, occorre considerare anche i seguenti fattori:

- tipo di violazione;
- natura, sensibilità e volume dei dati personali;
- facilità di associare i dati violati ad una persona fisica;
- gravità delle conseguenze per gli interessati;
- particolarità degli interessati (es. minori);
- particolarità degli autorizzati al trattamento (es. personale sanitario);
- numero degli interessati esposti al rischio.

	GRAVTA'		
PROBABILITA'	A	M	B
	M		
	B		

Tabella 2 – Gravità, Probabilità

C) appura se la violazione determina o meno l'obbligo di notifica e/o comunicazione al Garante, agli interessati e ad altre Autorità.

Sulla base della documentazione relativa alla segnalazione, **in relazione all'esito della valutazione del rischio**, il Titolare procederà nel seguente modo:

❖ ove risulti probabile che dalla violazione possano derivare rischi per i diritti e per le libertà degli interessati, provvederà a:

a) notificare il *data breach* all'Autorità di Controllo (art. 33 GDPR);

❖ ove risulti probabile che dalla violazione possano derivare **elevati rischi** per i diritti e le libertà degli interessati, provvederà a:

a) notificare il *data breach* all'Autorità di controllo (art. 33 GDPR);

b) comunicare il *data breach* ai soggetti cui si riferiscono i dati (c.d. Interessati) nei limiti e secondo quanto previsto dall'art. 34 GDPR;

❖ ove invece risulti improbabile che dalla violazione possano derivare rischi per i diritti e le libertà degli interessati, il Titolare del trattamento non procederà con le notifiche e comunicazioni di cui ai precedenti punti.

	DESCRIZIONE	NOTIFICA AL GARANTE	COMUNICAZIONE AGLI INTERESSATI
RISCHIO'	BASSO	NO	NO
	MEDIO	SI	NO
	ALTO	SI	SI

9.4 NOTIFICA ALL'AUTORITA' DI CONTROLLO

All'esito della valutazione, Il GDPR, ai sensi dell'art. 33, prevede che il Titolare del trattamento debba notificare all'Autorità di controllo una violazione di dati personali "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".

Pertanto gli eventuali atti di notifica all'Autorità di controllo e la possibile comunicazione all'/agli interessato/i da parte del Titolare del trattamento saranno predisposti e redatti con l'ausilio del DPO.

La comunicazione deve essere redatta con particolare cura ed attenzione in quanto potrebbe dar luogo ad un intervento dell'Autorità di controllo nell'ambito dei suoi compiti e poteri previsti dal Regolamento medesimo.

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.

Atteso che tale documentazione consente all'Autorità di Controllo di verificare in qualsiasi momento, il rispetto del GDPR in materia di *data breach*, la stessa sarà custodita, con la massima cura e diligenza, dal Titolare del trattamento il quale dovrà tenere apposito registro cronologico elaborato secondo variabili di interesse, dei casi di violazione dei dati.

Oltre il termine delle 72 ore, la notifica deve essere corredata anche delle ragioni del ritardo. È possibile comunicare successivamente all'Autorità Garante informazioni aggiuntive o dettagli rilevanti sulla violazione di cui il Titolare sia venuto a conoscenza, a seguito di ulteriori indagini.

Per quanto riguarda il caso particolare della indisponibilità temporanea o prolungata di dati personali dovuta ad indisponibilità del servizio che li tratta tra i fattori di valutazione deve essere incluso il tempo in cui i dati non sono disponibili. Se viene garantita la continuità operativa o il ripristino in tempi adeguati per scongiurare un danno per gli interessati, la notifica all'Autorità di controllo non è necessaria.

9.5 FORM DI NOTIFICA ALL'AUTORITA' DI CONTROLLO

La notifica all'Autorità di Controllo (il Garante per la Privacy ha espressamente previsto nel proprio sito web www.garanteprivacy.it una piattaforma ad hoc per le notifiche di *data breach*) conterrà necessariamente i seguenti dati:

- tipologia di incidente;
- descrizione del servizio impattato e/o della banca/banche dati oggetto di violazione di dati personali;
- intervallo temporale dell'incidente;
- luogo dell'incidente;
- misure tecniche di sicurezza applicate ai dati violati;
- misure attivate per il contenimento e la prevenzione;
- descrizione della 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;
- descrizione della probabile conseguenza della violazione dei dati personali;
- descrizione delle misure di sicurezza adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione di dati personali e anche, se del caso, per attenuarne i possibili effetti negativi;
- proposta di comunicazione di violazione di dati personali all'/agli interessato/i in base ad un'analisi dei dati oggetto di violazione (qualora la violazione sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche) e non ricorrendo alcuna delle condizioni di cui all'articolo 34, comma 3, del GDPR, che escludono la necessità di comunicazione della violazione all'interessato;
- il nome e i dati di contatto del Responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- i dati organizzativi di riferimento e i relativi recapiti dell'Istituto;
- il livello di gravità della violazione;
- l'eventuale comunicazione agli interessati e le relative modalità;
- qualora la notifica all'Autorità di Controllo non sia effettuata entro 72 ore, i motivi del ritardo.

9.6 COMUNICAZIONE AGLI INTERESSATI

Quando il rischio per l'interessato, valutato come specificato nel paragrafo 9.3, assume il valore Alto ("rischio elevato", GDPR art. 34), la violazione deve essere comunicata anche agli interessati.

Fanno eccezione i seguenti casi:

- i dati violati sono stati preventivamente protetti da misure tecniche e organizzative adeguate a scongiurare un rischio residuo elevato per gli interessati (ad esempio la cifratura o la pseudonimizzazione);
- i dati personali sono stati indisponibili per un periodo di tempo inferiore a 1 ora e non si è verificata alcuna altra tipologia di violazione;
- la comunicazione richiede un impegno spropositato. È il caso, ad esempio, di violazioni massive

di dati. In queste circostanze si può procedere a una comunicazione pubblica o di pari efficacia.

La comunicazione deve descrivere, con un linguaggio semplice e chiaro, la natura della violazione e deve inoltre contenere:
- il nome e i dati di contatto del Responsabile della protezione dei dati, del Titolare del trattamento o di altro contatto da cui ottenere maggiori informazioni;
- la descrizione delle probabili conseguenze della violazione;
- le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione e attenuarne i possibili effetti negativi.

A norma dell'art. 34, comma 3, non è richiesta la comunicazione all'interessato se:
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;
c) nel caso in cui la comunicazione diretta richieda uno sforzo ritenuto sproporzionato, si potrà utilizzare una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

9.7 REGISTRAZIONE DELLA VIOLAZIONE

Il Titolare del trattamento dei dati rappresentato dalla persona del Sindaco pro tempore, in caso di una violazione dei dati, deve procedere alla registrazione del *data breach* nell'apposito Registro delle violazioni (art.33, comma 5 del GDPR), da compilare secondo il modello allegato alla presente ed identificato come allegato B), documentando qualsiasi violazione dei dati personali, comprese le circostanze ad essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.
In caso di assenza di rischi per i dati personali, deve annotare e documentare i motivi della mancata notifica al Garante Privacy in modo da comprovare la effettiva assenza dei rischi.
Tutta la documentazione relativa alle segnalazioni deve essere archiviata.

9.8 RECEPIMENTO DI EVENTUALE RISPOSTA DEL GARANTE

Il Titolare dispone ulteriori indagini o eventuali misure correttive, secondo le disposizioni ricevute dal Garante.

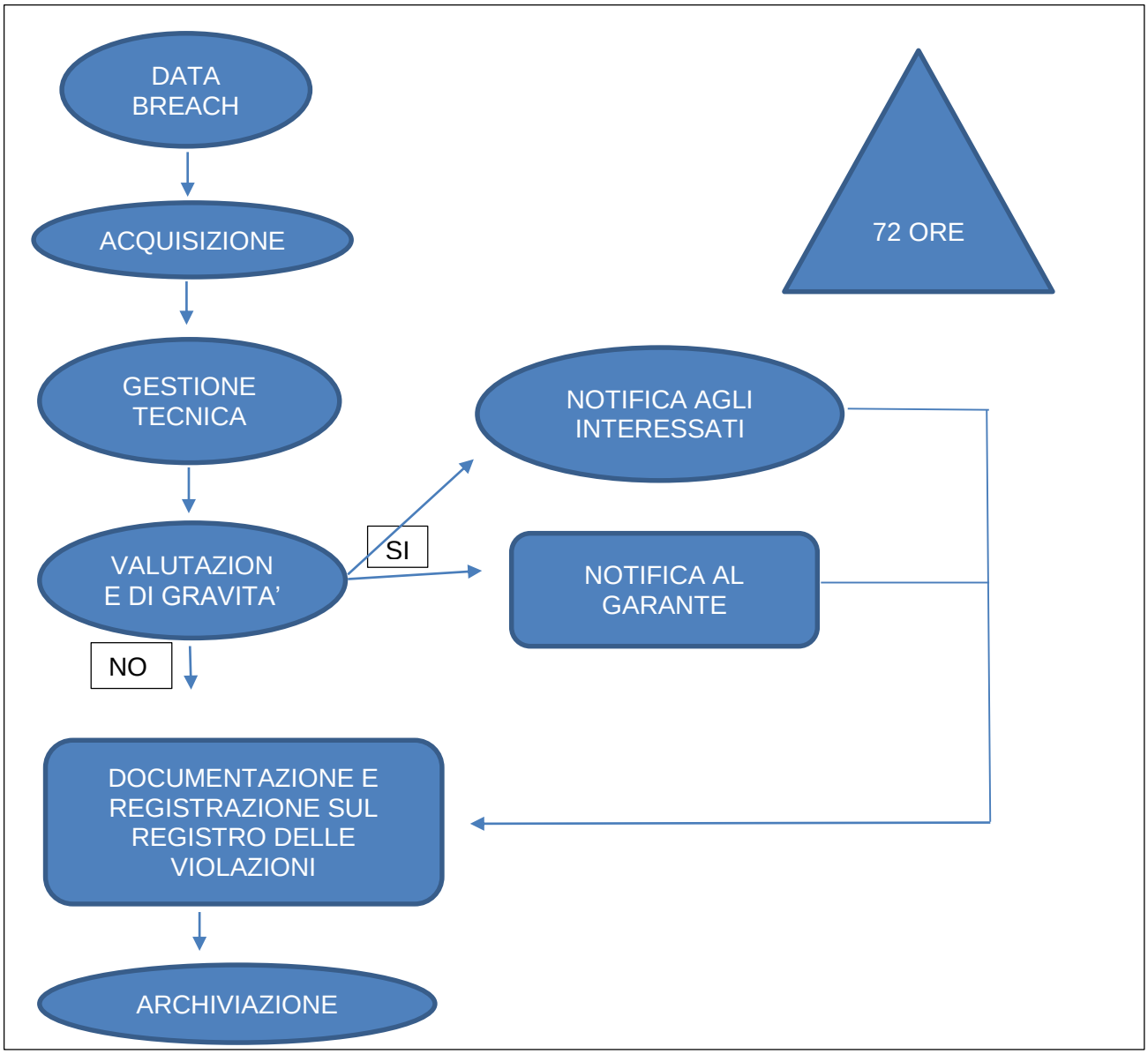
9.9 SEGNALAZIONE AD ALTRE AUTORITA'

Il Titolare, qualora necessario, comunica la violazione di dati alle altre Autorità competenti (Autorità giudiziaria, ecc.), a mezzo gli Uffici del Comune Breda di Piave preposti.

9.10 GESTIONE DEL *DATA BREACH* ESTERNO AL COMUNE DI BREDA DI PIAVE

Il Responsabile del Trattamento ex art. 28 del GDPR è tenuto ad osservare la presente procedura di gestione del *data breach* e ad informare il Titolare del trattamento senza ingiustificato ritardo di ogni potenziale evento di violazione dei dati.
La segnalazione del *data breach* dovrà essere inviata agli indirizzi indicati nell'atto di nomina al Titolare del trattamento.

9.11 SCHEMA SINTESI FASI PROCEDURA



10. DIFFUSIONE DELLA PROCEDURA

La presente procedura dovrà essere divulgata in modo capillare e dovrà essere pubblicata sul sito internet del Comune Breda di Piave in Amministrazione Trasparente, sezione Altri contenuti-privacy.

Appendice 1 – Acronimi e Glossario

Autorità di controllo (o autorità Garante)	L'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del GDPR.
Data breach (o violazione di dati personali)	"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" (GDPR, art. 4 punto 12).
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" (GDPR, art. 4 punto 1).
Danno	Conseguenza negativa derivante dal verificarsi di una determinata minaccia; il danno può qualificarsi come materiale quando determina una concreta lesione all'ambito fisico o patrimoniale dell'interessato oppure immateriale quando riguarda le possibili conseguenze dannose derivanti dal trattamento di dati personali, di natura non patrimoniale e che affliggono la sfera interiore del soggetto interessato.
Responsabile della protezione dei dati o DPO	Soggetto cui è attribuito dal Titolare del trattamento il compito di informare e fornire consulenza sugli obblighi derivanti dal GDPR e di sorvegliarne l'osservanza. Fornisce, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati (PIA) e ne sorveglia lo svolgimento. Coopera con l'Autorità di controllo e funge da punto di contatto con essa (GDPR, art. 37, 38, 39).
GDPR	Regolamento Ue n. 679/2016 "General Data Protection Regulation", in italiano indicato come "Regolamento generale sulla protezione dei dati".
Interessato	La persona fisica cui si riferiscono i dati personali.
Minaccia	Una serie di eventi dannosi che possono compromettere le caratteristiche di integrità, riservatezza e disponibilità del dato personale.
Misura di sicurezza	Accorgimento tecnico e organizzativo utilizzato per garantire che i dati non vadano distrutti o persi anche in modo accidentale, per garantire che solo le persone autorizzate possano avere accesso ai dati e che non siano effettuati trattamenti contrari alle norme di legge o diversi da quelli per cui i dati erano stati raccolti.

Privacy Impact Assessment (PIA)	Valutazione d'impatto che deve essere compiuta dal titolare quando "un tipo di trattamento (…) può presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (GDPR, art. 35).
Responsabile del trattamento	La persona fisica o giuridica, l'autorità pubblica o altro organismo che tratta dati personali per conto del titolare del trattamento.
Servizio ICT	Insieme di funzionalità informatiche omogenee destinate a supportare un processo o un'attività lavorativa. Un servizio informatico è composto da una o più applicazioni software e dalla relativa infrastruttura tecnologica di supporto.
Titolare del trattamento	La persona fisica o giuridica, l'autorità pubblica o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali.
Trattamento	Operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati, applicate a dati personali, come la raccolta, la registrazione, la conservazione, la modifica, l'estrazione, la consultazione, l'uso, la comunicazione, la distruzione, ecc.

Appendice 2 – Categorie di dati personali

Dati personali comuni	
Anagrafici	Dati personali anagrafici quali nome, cognome, data e luogo di nascita, stato civile, residenza.
Contabili, fiscali, inerenti possidenze e riscossione	Dati personali quali versioni parziali/integrali di documenti contabili, dati di dettaglio risultanti dalle dichiarazioni fiscali oppure dai cedolini dello stipendio di ciascun lavoratore, indicazioni di dati riferiti a percettori di somme (e.g. i recapiti individuali e le coordinate bancarie utilizzate per effettuare i pagamenti), complesso dei beni posseduti (e.g case, terreni, altre proprietà).
Inerenti il rapporto di lavoro	Dati personali inerenti l'esecuzione del rapporto di lavoro: tipologia di contratto e livello contrattuale, dettagli di assunzione, irrogazione di sanzioni disciplinari, stipendio, trasferimenti del lavoratore, etc.
Tracciamenti	Dati personali presenti nei tracciati record generati dalla registrazione delle operazioni svolte su sistemi, applicativi, ecc.
Dati inerenti situazioni giudiziarie civili, amministrative, tributarie	Trattamento di dati personali quali cartelle tributarie, pagamenti, rateizzazioni, procedure in corso, assenza o esistenza di condanne emesse, contenziosi pendenti.
Dati personali (comuni) specifici	
Dati che consentono geolocalizzazione	Dati personali derivanti dalla rilevazione di coordinate satellitari relative alla geolocalizzazione di apparati elettronici di tipo radio mobili e veicolari, celle territoriali agganciate dai ricevitori GPS, dati relativi agli indirizzi IP.
Audio/video/foto	Audio, video, fotogrammi, immagini che possano far riconoscere, tramite riconoscimento facciale, vocale e/o comportamentale, la persona fisica.
Dati di profilazione	Dati riguardanti aspetti personali relativi a una persona fisica, che ne consentano di identificare preferenze, interessi, analizzare o prevedere il rendimento professionale, la situazione economica, la salute, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti del soggetto.
Dati personali finanziari	
Dati relativi all'esistenza di rapporti finanziari (coordinate bancarie, consistenze saldi, movimenti, giacenza media, etc.)	Dati relativi alla situazione bancaria attuale e/o passata dell'interessato, informazioni gestite da operatori finanziari quali: i saldi iniziali e finali del rapporto, il totale dei movimenti annuali in entrata e in uscita, la c.d. giacenza annuale media etc.

Dati personali particolari	
Convinzioni religiose o filosofiche/opinioni politiche/origine razziale/adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale	Dati personali che possano rivelare convinzioni religiose o filosofiche/opinioni politiche/origine razziale/adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale.
Stato di salute, assistenza sanitaria, orientamento/vita sessuale	Attinenti: - lo stato di salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, dati idonei a rivelare informazioni relative al suo stato di salute, ad esempio, certificato medico, cartella clinica, etc. - l'orientamento sessuale e/o la vita sessuale della persona fisica
Genetici	Dati personali relativi alle caratteristiche genetiche, ereditarie o acquisite, di una persona fisica, che risultino dall'analisi di un campione biologico della persona fisica in questione.
Dati personali biometrici	
Impronte digitali	Dati personali relativi ad impronte digitali e caratteristiche della topografia della mano, utilizzate per l'identificazione degli esseri umani.
Altre caratteristiche biometriche	Dati relativi ad altre caratteristiche fisiche quali: retina, vascolarizzazione, forma del volto. Possono intendersi caratteristiche biometriche anche caratteristiche comportamentali quali impronta vocale, movimenti del corpo, stile di battitura sulla tastiera.
Firma grafometrica	Firma grafometrica, analoga alla firma “olografa”, inserita in un'apposita tavoletta elettronica con l'ausilio di una penna elettronica.
Dati personali giudiziari	
Casellario giudiziale	Dati contenuti all'interno del certificato penale del casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione).
Qualità di indagato/imputato o altre situazioni giudiziarie e reati o connesse misure di sicurezza	Dati idonei a rivelare che un determinato soggetto è stato sottoposto ad indagini di polizia giudiziaria, al termine delle quali, è stato accusato di un reato nell'ambito di un Procedimento penale (certificato dei carichi pendenti).

ALLEGATO A

MODULO DI COMUNICAZIONE *DATA BREACH*

Da inviare a - segreteria@comunebreda.it
- e-mail del DPO*
- protocollo.comune.bredadipiave.tv@pecveneto.it

Io sottoscritto _____
in qualità di _____
dichiaro quanto segue:

Data dell'incidente	○ Data_____ ○ Tra il_____ed il _____ ○ In un tempo non ancora determinato ○ Ancora in corso
Data in cui si è venuti a conoscenza dell'evento	
Luogo della violazione **(Indicare la Area/Ufficio..)**	○ Luogo _____ ○ Area _____ ○ Ufficio _____
Nome della persona che ha riferito della violazione	
Dati di contatto della persona che ha riferito della violazione (indirizzo e-mail, numero telefonico)	
Breve descrizione della violazione di dati personali	
Specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili, ecc.	
Modalità di esposizione al rischio **Tipo 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:

Dispositivo oggetto della violazione	○ Computer ○ Dispositivo mobile ○ Documento cartaceo ○ File o parte di un file Strumento di backup ○ Rete ○ Altro:
Categoria e numero approssimativo degli Interessati colpiti dalla violazione di dati personali	○ Categoria _____ ○ N._____di persone ○ Circa_____persone ○ Un numero (ancora) sconosciuto di persone
Tipologia di dati coinvolti nella violazione	○ Dati anagrafici ○ Numero di telefono (fisso o mobile) ○ Indirizzo di posta elettronica ○ Dati di accesso e di identificazione (user name, password, customer ID, altro) ○ Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro) ○ Altri dati di personali (sesso, data di nascità, età, ...), ○ dati sensibili e giudiziari ○ Ancora sconosciuto
Livello di gravità della violazione dei dati personali (secondo le valutazioni dell' Area/Ufficio)	○ Basso/trascurabile ○ Medio ○ Alto
Misure tecniche e organizzative applicate ai dati colpiti dalla violazione	

Luogo, Data, FIRMA_____

* **disponibile sito istituzionale in Amministrazione Trasparente sezione Altri Contenuti- Privacy.**

ALLEGATO B

REGISTRO DATA BREACH

COMUNE DI BREDA DI PIAVE

Via Trento e Trieste, 26, 31030 Breda di Piave (TV)
P.Iva 00559560263 CF 80006200267

N° prog.	Data della violazione	Luogo della violazione (Struttura…)	Descrizione della violazione	Tipologia della violazione	Categorie di interessati e numero approssimativo	Categorie di dati personali e numero approssimativo	Cause della violazione	Conseguenze della violazione	Misure correttive, responsabilità e data di attuazione	Gravità	Probabilità	Rischio	Necessità di notifica al Garante e data	Necessità di comunicazione agli interessati e data	Motivazioni della mancata notifica o comunicazione	Verifica attuazione misure e data	Verifica efficacia misure e data di verifica