UNIONE DEI COMUNI DELLA VALLE USTICA

CITTA'METROPOLITANA DI ROMA CAPITALE

Deliberazione COPIA Giunta dell'Unione

Atto n.09/2026

OGGETTO: " Procedura operativa interna per la gestione delle violazioni di dati personali (Data Breach) **".**

L'anno duemilaventisei questo giorno 19 marzo alle ore 11.00 nella Sede dell'Unione si è riunita

LA GIUNTA DELL'UNIONE DEI COMUNI DELLA VALLE USTICA

NOME COGNOME	**PRESENTE**	**ASSENTE**
Marco Bernardi	SI	
Claudio Giustini		SI
Ilaria Passacantilli	SI	
Claudio Pettinelli		SI
Laura Mattiucci	SI	

Presiede la Sig.ra Ilaria Passacantilli PRESIDENTE

Assiste il Segretario Dott. Guido Mazzocco.
Risultato legale il numero dei convenuti il Presidente dichiara aperta la discussione per deliberare sull'oggetto sopraindicato.

Il PRESIDENTE
F.to Ilaria Passacantilli

IL SEGRETARIO
F.to Dott. Guido Mazzocco

DICHIARAZIONE DI PUBBLICAZIONE
Si dichiara che copia della deliberazione sopraestesa, è pubblicata nel sito web istituzionale dal 26/03/2026 e vi rimarrà per 15 giorni consecutivi.
Vicovaro,26/03/2026

Il Segretario
f.to Dott. Guido Mazzocco

TRASMISSIONI E COMUNICAZIONI
La presente deliberazione è stata:
( ) Comunicata, con lettera n in data Ai Signori Capigruppo Consiliari

Vicovaro,

Il Segretario
F.to Dott. Guido Mazzocco

COPIA CONFORME ALL'ORIGINALE PER USO AMMINISTRATIVO
Vicovaro,26/03/2026

Il Segretario
Dott. Guido Mazzocco

Allegato alla deliberazione della Giunta dell'Unione dei Comuni della Valle Ustica
n. 09/2026

PARERE DI REGOLARITA' TECNICA/AMMINISTRATIVA

Ai sensi del D.Lvo 267/00, recante il Testo Unico delle leggi sull'Ordinamento degli Enti Locali, esprime parere favorevole in ordine alla regolarità TECNICA/AMMINISTRATIVA

IL SEGRETARIO
f.to Dott.Guido Mazzocco

19.03.2026

LA GIUNTA UNIONALE

Premesso che nell'allegato sono riportati i riferimenti normativi e le motivazioni per cui si rende necessario provvedere in merito;

Visti:

il D.P.R. n. 445/2000, con cui è stata unificata e coordinata tutta la normativa in materia di documentazione amministrativa;

lo Statuto e il TUEL;

il parere di regolarità tecnica, rilasciato dal competente Responsabile di servizio, ai sensi dell'art. 49, allegato alla presente ;

il D.Lgs. n. 196/2003 recante il Codice in materia di protezione dei dati personali e il Regolamento UE 2016/679 (GDPR) ;

il D.Lgs. 82/2005 e ss. mm. ii. (Codice dell'Amministrazione Digitale) (modificato e integrato con il D.Lgs. n. 179/2016 e il D.Lgs. n.217/2017);

Dato atto:

Visto lo schema di "Manuale " allegato alla presente deliberazione per costituirne parte integrante e sostanziale, di cui si condividono contenuti e finalità;

Con votazione unanime e palese,

DELIBERA

Di approvare la procedura operativa interna per la gestione delle violazioni di dati personali (Data Breach) ;

Di dichiarare la presente deliberazione, stante l'urgenza di provvedere, immediatamente eseguibile, ai sensi dell'art. 134, comma 4, del D.Lgs. 267/2000, con separata votazione unanime e favorevole.

PROCEDURA OPERATIVA INTERNA PER LA GESTIONE DELLE VIOLAZIONI DI DATI PERSONALI (DATA BREACH)6

Sommario

PROCEDURA OPERATIVA INTERNA PER LA GESTIONE DELLE VIOLAZIONI DI DATI PERSONALI (DATA BREACH) ... 6

Introduzione normativa ed esplicativa sul data breach nella Pubblica Amministrazione 6

Definizione e tipologie di data breach nel contesto dellA VITA DELL'Ente 7
Distinzione tra incidente di sicurezza e violazione dei dati 7
Classificazione delle violazioni 7
Tipologia dei dati e trattamenti compromessi nell'Ente 7
Tempistiche e modalità di notifica: flussi interni e comunicazioni esterne 8
Il flusso di notifica interno 8
Notifica al Garante della Privacy: procedura telematica 9
Analisi degli impatti, valutazione del danno e comunicazione agli interessati 9
Metodologia di valutazione del rischio 10
Comunicazione agli interessati: quando e come 10
DEFINIZIONE DEL PIANO D'INTERVENTO 10
Il Registro delle violazioni: obblighi di documentazione e conservazione 11
Struttura del Registro 11
Profili di responsabilità e sanzioni nel settore pubblico 12
Responsabilità amministrativa e sanzioni del Garante 12
Responsabilità erariale (Corte dei Conti) 12
Responsabilità disciplinare e penale 13

PROCEDURA OPERATIVA INTERNA PER LA GESTIONE DELLE VIOLAZIONI DI DATI PERSONALI (DATA BREACH)

L'attuale scenario digitale e l'incremento esponenziale delle minacce informatiche, uniti alla crescente complessità dei trattamenti di dati personali svolti dalla Pubblica Amministrazione, impongono agli Enti l'adozione di protocolli rigorosi per la gestione degli incidenti di sicurezza. La presente procedura operativa definisce le linee guida metodologiche, giuridiche e tecniche per l'identificazione, la valutazione, la notifica e la documentazione delle violazioni di dati personali (data breach), in piena conformità al Regolamento UE 2016/679 (GDPR), al D.Lgs. 196/2003 (Codice Privacy) e alle più recenti indicazioni delle autorità di controllo.

Introduzione normativa ed esplicativa sul data breach nella Pubblica Amministrazione

Il quadro normativo che disciplina la gestione delle violazioni dei dati personali si fonda sul principio di responsabilizzazione (accountability), che permea l'intera struttura del Regolamento Generale sulla Protezione dei Dati (GDPR). Per un Ente, il rispetto di tale principio non si esaurisce nella mera conformità formale, ma richiede la capacità di dimostrare in ogni momento l'adeguatezza delle misure tecniche e organizzative adottate per garantire la sicurezza dei trattamenti.

L'articolo 33 del GDPR introduce l'obbligo per il Titolare del trattamento di notificare la violazione dei dati personali all'autorità di controllo competente – in Italia, il Garante per la protezione dei dati personali – a meno che sia improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche. Parallelamente, l'articolo 34 impone l'obbligo di comunicazione all'interessato qualora la violazione sia suscettibile di presentare un rischio elevato. Tale architettura normativa è integrata a livello nazionale dal D.Lgs. 30 giugno 2003, n. 196, così come modificato dal D.Lgs. 10 agosto 2018, n. 101, che specifica le modalità di attuazione e i profili sanzionatori nel contesto italiano.

Il Comitato Europeo per la Protezione dei Dati (EDPB) ha fornito interpretazioni essenziali attraverso le Linee Guida 9/2022 sulla notifica delle violazioni, che sostituiscono le precedenti indicazioni del Gruppo di lavoro Articolo 29 (WP250). Queste linee guida chiariscono che il termine delle 72 ore per la notifica decorre dal momento in cui il Titolare ha "conoscenza" della violazione, ovvero quando ha un grado ragionevole di certezza che si sia verificato un incidente di sicurezza che ha compromesso dati personali.

Nelle Pubbliche Amministrazioni, la gestione del data breach assume una connotazione particolare a causa della natura istituzionale delle finalità perseguite. Gli Enti trattano dati personali per l'esecuzione di compiti di interesse pubblico o connessi all'esercizio di pubblici poteri, ai sensi dell'articolo 6, paragrafo 1, lett. e) del GDPR. Questo status implica che la perdita di integrità o riservatezza dei dati non rappresenti solo una violazione normativa, ma possa compromettere l'erogazione di servizi essenziali e ledere la fiducia del cittadino nelle istituzioni.

Le autorità di controllo, nelle loro analisi, pongono l'accento sulla necessità che l'Ente sia in grado di rilevare tempestivamente l'evento. L'articolo 32 del GDPR sottolinea che le misure di sicurezza devono essere adeguate al rischio, tenendo conto dello stato dell'arte, dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento. Per una Amministrazione, ciò si traduce nell'obbligo di implementare sistemi di monitoraggio capaci di intercettare accessi abusivi, malware o anomalie nel traffico di rete che potrebbero indicare

un'esfiltrazione di dati.

Definizione e tipologie di data breach nel contesto dellA VITA DELL'Ente

Una corretta gestione operativa richiede innanzitutto la capacità di distinguere e classificare l'evento occorso. La normativa definisce la violazione dei dati personali come una 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.

Distinzione tra incidente di sicurezza e violazione dei dati

È fondamentale per il personale dell'Ente comprendere la differenza tra un incidente di sicurezza informatica e un data breach. Sebbene ogni violazione di dati personali sia originata da un incidente di sicurezza, il contrario non è necessariamente vero. Un incidente di sicurezza è un evento che può compromettere la disponibilità, l'integrità o la riservatezza di un sistema o di una rete. Se tale incidente coinvolge sistemi che non contengono dati personali (ad esempio, un server dedicato esclusivamente alla gestione del traffico semaforico senza identificazione dei veicoli), si configura un incidente di sicurezza ma non una violazione ai sensi del GDPR.

Classificazione delle violazioni

Le violazioni possono essere classificate in tre categorie principali, che possono anche sovrapporsi nello stesso evento:

1. Violazione della riservatezza (Confidentiality breach): si verifica quando si ha una divulgazione o un accesso a dati personali non autorizzato o accidentale. Esempi tipici in un Ente includono l'invio di una mail con dati sensibili a un destinatario sbagliato o la pubblicazione erronea di un atto integrale online sul sito web ufficiale senza l'oscuramento dei dati eccedenti.

2. Violazione dell'integrità (Integrity breach): consiste nell'alterazione non autorizzata o accidentale di dati personali. Un esempio potrebbe essere la modifica dolosa dei record relativi ai pagamenti dei tributi locali o la corruzione accidentale di un database anagrafico che renda i dati inesatti.

3. Violazione della disponibilità (Availability breach): si ha quando si verifica la perdita, la distruzione o l'accesso accidentale o non autorizzato che impedisce l'utilizzo dei dati personali in caso di necessità. L'esempio più critico e frequente è l'attacco ransomware, che cripta i server rendendo i dati indisponibili fino al ripristino o al pagamento del riscatto (pratica quest'ultima fortemente sconsigliata).

Tipologia dei dati e trattamenti compromessi nell'Ente

L'Ente gestisce una varietà di banche dati che presentano profili di rischio differenziati. La valutazione dell'impatto di un data breach deve tenere conto della specifica natura dei dati coinvolti.

Tipologia di Dati	**Descrizione ed Esempi**	**Esempi di Trattamenti Coinvolti**
Dati Comuni	Nome, cognome, indirizzo,	Anagrafe, protocollo, gestione

	codice fiscale, numero di telefono, e-mail.	tributi, contratti.
Categorie Particolari	Dati sanitari, opinioni politiche, orientamento religioso o sessuale, dati biometrici.	Servizi sociali, contributi economici, assistenza handicap, medicina del lavoro, risorse umane.
Dati Giudiziari	Informazioni su condanne penali, reati o connesse misure di sicurezza.	Polizia Locale (sanzioni), ufficio procedimenti disciplinari, appalti.
Dati Finanziari	Coordinate bancarie (IBAN), reddito, ISEE, situazioni debitorie.	Ragioneria, pagamenti fornitori, rimborsi fiscali, agevolazioni sociali.
Dati Comportamentali	Dati di localizzazione (GPS), traffico telematico, abitudini d'uso.	Monitoraggio flotta mezzi comunali, log di accesso alla rete WiFi pubblica.

Tempistiche e modalità di notifica: flussi interni e comunicazioni esterne

La tempestività è il fattore determinante nella gestione delle violazioni. L'obbligo di agire entro le 72 ore richiede un'organizzazione interna collaudata che eviti rallentamenti burocratici.

Il flusso di notifica interno

Ogni dipendente, stagista, collaboratore o amministratore che rilevi un'anomalia o un possibile incidente deve segnalarlo immediatamente, senza attendere di avere la certezza assoluta che si tratti di una violazione. La procedura interna prevede i seguenti passaggi:

1. Rilevazione: l'incaricato rileva l'evento (es. ricezione di un messaggio di riscatto ransomware, smarrimento di un faldone di documenti cartacei, notifica di errore di invio e-mail a destinatari massivi).

2. Segnalazione Immediata: il soggetto invia una comunicazione urgente al proprio Responsabile di riferimento, il quale informa immediatamente il Servizio Interno Privacy, il Responsabile della Protezione Dati (RPD/DPO) dell'Ente e per conoscenza al Titolare del trattamento.

3. Analisi Preliminare: il Dirigente/Responsabile del settore coinvolto insieme al Servizio Interno Privacy, avvalendosi se necessario del Responsabile della Transizione Digitale (RTD), effettua un'analisi rapida per confermare la natura dell'evento e raccogliere i primi dati (numero di interessati, tipologia di dati coinvolti).

4. Coinvolgimento del RPD: l'RPD riceve la documentazione preliminare e fornisce consulenza al Responsabile del Servizio Interno Privacy e al Titolare (legale rapresentante o suo delegato) sulla necessità di procedere alla notifica al Garante e alla comunicazione agli interessati.

5. Decisione del Titolare: il Titolare, sulla base del parere del Servio Interno Privacy e dell'RPD, autorizza formalmente la notifica esterna.

In caso di violazione subita da un Responsabile Esterno del Trattamento (es. il fornitore del software per la gestione dei tributi o l'azienda che gestisce l'hosting del sito web comunale), quest'ultimo ha l'obbligo contrattuale e normativo di informare il Titolare "senza ingiustificato ritardo". Gli accordi per il trattamento dei dati (DPA ex art. 28 GDPR) dovrebbero prevedere un termine ancora più breve (es. 24/48 ore) per consentire all'Ente di rispettare il proprio termine delle 72 ore.

Notifica al Garante della Privacy: procedura telematica

Se la violazione comporta un rischio per i diritti e le libertà delle persone fisiche, l'Ente deve notificarla al Garante Privacy. La notifica deve avvenire esclusivamente tramite la procedura telematica disponibile sul portale dell'Autorità.

La procedura sul sito web del Garante (https://servizi.gpdp.it/databreach/s/) si articola nelle seguenti fasi operative:

- Accesso e Autenticazione: l'utente (rappresentante legale o soggetto delegato) accede tramite identità digitale (SPID, CIE, CNS). È disponibile anche una modalità non autenticata, ma richiede passaggi aggiuntivi di verifica via e-mail.
- Compilazione del Modulo: il sistema guida il dichiarante nell'inserimento di informazioni specifiche:
  - Sezione A: dati identificativi del Titolare del trattamento.
  - Sezione B: dettagli della violazione (data e ora dell'evento, momento della scoperta, modalità di conoscenza, motivi dell'eventuale ritardo oltre le 72 ore).
  - Sezione B1: integrazione di una notifica precedente (nel caso in cui la prima notifica sia stata inviata in forma preliminare).
  - Natura e Causa: classificazione tra perdita di riservatezza, integrità o disponibilità e descrizione dell'incidente (es. errore umano, attacco cyber, furto fisico).
  - Interessati e Dati: indicazione delle categorie di persone colpite (dipendenti, utenti, minori, ecc.) e del volume approssimativo dei dati.
  - Misure di Sicurezza: descrizione delle misure tecniche e organizzative adottate prima della violazione per proteggere i dati e di quelle implementate post-evento per mitigare i danni.
- Finalizzazione: il sistema genera un file PDF che riassume i dati inseriti. Tale file deve essere scaricato, firmato digitalmente in formato CAdES-p7m (senza marche temporali) e ricaricato sul portale.
- Ricezione Fascicolo: una volta trasmessa, la procedura assegna un numero di fascicolo e un PIN, necessari per qualsiasi successiva integrazione o comunicazione con l'Autorità.

È importante sottolineare che la notifica può essere effettuata in fasi successive. Qualora non sia possibile fornire tutte le informazioni entro le 72 ore, il Titolare può inviare una prima notifica parziale, specificando che ulteriori dettagli verranno forniti non appena disponibili.

Analisi degli impatti, valutazione del danno e comunicazione agli interessati

Una violazione non deve essere notificata o comunicata automaticamente: è necessaria una valutazione del rischio rigorosa. Il GDPR distingue tra "rischio" (che obbliga alla notifica al Garante) e "rischio elevato" (che obbliga anche alla comunicazione anche agli interessati).

Metodologia di valutazione del rischio

La valutazione della gravità del rischio si basa su un'analisi multidimensionale:

1. Contesto del Trattamento: si valuta la criticità dei dati coinvolti. I dati anagrafici semplici hanno un punteggio base basso, mentre dati sanitari, giudiziari o relativi a minori portano a un incremento significativo del punteggio di gravità.
2. Facilità di Identificazione: indica quanto sia semplice risalire all'identità dell'individuo partendo dai dati violati. Il rischio aumenta se i dati non sono cifrati o pseudonimizzati in modo efficace.
3. Circostanze della Violazione: considera le modalità dell'evento. Un attacco cyber intenzionale con esfiltrazione di dati ha un peso maggiore rispetto allo smarrimento di un documento cartaceo all'interno di un'area protetta dell'ufficio.

Il calcolo della gravità finale permette di classificare l'evento in quattro livelli (Basso, Medio, Alto, Molto Alto), definendo di conseguenza le azioni obbligatorie.

Comunicazione agli interessati: quando e come

La comunicazione all'interessato è finalizzata a permettergli di adottare precauzioni per proteggersi dalle possibili conseguenze della violazione. Deve essere effettuata senza ingiustificato ritardo quando il rischio è classificato come "elevato".

Il contenuto della comunicazione deve essere chiaro, trasparente e privo di tecnicismi eccessivi, includendo:

- Una descrizione della natura della violazione.
- I recapiti del DPO per ottenere ulteriori informazioni.
- Le probabili conseguenze negative (es. rischio di furto d'identità, phishing mirato, accessi abusivi a conti correnti).
- Le misure adottate dall'Ente per rimediare.
- Raccomandazioni specifiche per l'interessato (es. cambiare le password dei propri account personali se simili a quelle violate, prestare attenzione a e-mail sospette, bloccare carte di pagamento coinvolte).

La comunicazione deve essere individuale (e-mail, PEC, lettera, SMS). Tuttavia, se questa comportasse uno sforzo sproporzionato per l'Ente (ad esempio, se gli interessati sono decine di migliaia o se i recapiti non sono aggiornati), è possibile procedere a una comunicazione pubblica di pari efficacia, come la pubblicazione in evidenza sulla home page del sito istituzionale dell'Ente o tramite comunicati stampa sui media locali.

DEFINIZIONE DEL PIANO D'INTERVENTO

Una volta concluso il processo di notifica e comunicazione della violazione di dati personali agli interessati, il soggetto che esercita le funzioni di titolare del trattamento, supportato dal RPD, svolge le seguenti attività:

- Analizza le cause che hanno determinato la violazione di dati personali;
- Valuta le opportunità di miglioramento dei presidi e dei processi di monitoraggio delle violazioni dei dati personali, al fine di mettere in atto misure tecniche e organizzative adeguate a garantire il rispetto del Regolamento;
- Definisce un piano di rimedio al fine di garantire un livello di sicurezza adeguato ai rischi in ordine alla protezione dei dati personali trattati.

Per ciascuna violazione di dati personali, il Titolare del trattamento è tenuto a verificare se l'incidente è il risultato di un errore umano o di un problema di natura tecnica o organizzativa e valutare misure correttive volte a prevenire il ripetersi dell'evento. Il titolare del trattamento poi, insieme ai responsabili interni di riferimento e con il supporto del RPD, deve monitorare quelle violazioni che sono state preventivamente verificate e che hanno maggiore probabilità di verificarsi, in modo da applicare azioni correttive specifiche al fine di limitare la massimo eventuali impatti negativi.

Il Registro delle violazioni: obblighi di documentazione e conservazione

L'articolo 33, paragrafo 5 del GDPR impone al Titolare del trattamento di documentare qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione deve essere conservata dall'Ente e messa a disposizione del Garante in caso di controlli o ispezioni.

Struttura del Registro

Il Registro non deve limitarsi a elencare le violazioni notificate al Garante, ma deve includere anche tutti i "falsi positivi" e gli incidenti di sicurezza che sono stati valutati come "non a rischio" e per i quali non si è proceduto alla notifica esterna. Questa completezza serve a dimostrare all'Autorità che l'Ente monitora attivamente i propri sistemi e compie analisi di rischio ponderate.

Di seguito si riporta l'esempio di schema operativo del registro che l'Ente è tenuto a compilare e aggiornare costantemente.

Campo del Registro	**Descrizione e Note Operative**	**Dati dell'Evento**
ID Violazione	Codice univoco assegnato internamente (es. DB-202X-001).	
Data e Ora Evento	Momento esatto o presunto dell'accadimento della violazione.	
Data e Ora Conoscenza	Momento in cui l'Ente è venuto a conoscenza dell'evento.	
Descrizione della Violazione	Sintesi delle circostanze (es. attacco SQL injection, smarrimento chiavetta USB).	
Categoria di Dati	Elenco delle tipologie di dati coinvolti (anagrafici, sanitari, giudiziari, ecc.).	
Categoria di Interessati	Tipologia di persone colpite (dipendenti, cittadini residenti, minori, fornitori).	

Volume Dati/Interessati	Numero approssimativo di record e di persone fisiche coinvolte.	
Valutazione del Rischio	Esito del risk assesment (Basso, Medio, Alto, Molto Alto) con motivazione sintetica.	
Notifica al Garante	Indicazione (SI/NO), data di invio e numero di protocollo della notifica.	
Comunicazione Interessati	Indicazione (SI/NO), data e canale utilizzato per informare i soggetti colpiti.	
Misure di Mitigazione	Elenco delle azioni correttive e preventive adottate per evitare il ripetersi dell'evento.	
Esito e Chiusura	Stato della gestione (In corso/Chiuso) e data di risoluzione definitiva dell'incidente.	

Il Registro deve essere gestito preferibilmente in formato elettronico protetto (es. file excel cifrato o database dedicato) con accesso limitato al DPO, al Segretario Generale e ai referenti dell'Ufficio Interno Privacy.

Profili di responsabilità e sanzioni nel settore pubblico

La gestione inadeguata di un data breach espone l'Ente e i suoi vertici a gravi rischi legali, finanziari e reputazionali.

Responsabilità amministrativa e sanzioni del Garante

Il Garante Privacy ha il potere di irrogare sanzioni amministrative pecuniarie elevate. Per le violazioni degli obblighi di sicurezza (Art. 32) e di notifica/comunicazione (Artt. 33 e 34), le sanzioni possono arrivare fino a 10 milioni di euro. Sebbene per gli Enti Pubblici l'Autorità tenda a calibrare le sanzioni in base alla gravità e alla cooperazione mostrata, provvedimenti recenti hanno visto Comuni sanzionati con decine di migliaia di euro per omessa protezione di dati sanitari o pubblicazioni illecite.

Responsabilità erariale (Corte dei Conti)

Uno dei profili più critici per i Dirigenti/Responsabili, per il Segretario Generale e per gli Amministratori è il rischio di danno erariale. Qualora l'Ente sia costretto a pagare una sanzione amministrativa al Garante a causa di una condotta gravemente colposa del dipendente o del Responsabile (es. mancato aggiornamento di sistemi obsoleti, assenza di backup funzionanti o ritardo ingiustificato nella notifica), la Procura della Corte dei Conti può avviare un procedimento per rivalersi sul patrimonio personale del responsabile. La giurisprudenza contabile ha stabilito

che la violazione dei generali doveri di diligenza e cautela, connaturati alla funzione dirigenziale, integra la colpa grave necessaria per l'addebito del danno.

Responsabilità disciplinare e penale

Ai sensi del D.Lgs. 165/2001 e dei CCNL di comparto, l'omessa segnalazione di un incidente di sicurezza o il mancato rispetto delle procedure interne di protezione dati costituisce un illecito disciplinare. Le sanzioni possono variare dal richiamo scritto alla sospensione dal servizio, fino al licenziamento nei casi di dolo o colpa gravissima che abbiano arrecato un grave danno all'Ente o a terzi. Sotto il profilo penale, l'accesso abusivo a un sistema informatico (Art. 615-ter c.p.) e la rivelazione di segreti d'ufficio (Art. 326 c.p.) rimangono le fattispecie di riferimento in caso di condotte illecite dei dipendenti.

In conclusione, la presente procedura operativa costituisce lo strumento cardine per garantire che l'Ente non sia solo una vittima passiva degli incidenti di sicurezza, ma un soggetto attivo e responsabile, capace di proteggere i diritti fondamentali dei propri cittadini attraverso una gestione strutturata, trasparente e tempestiva di qualsiasi violazione di dati personali.