PROVINCIA DI FOGGIA

PROCEDURA PER LA GESTIONE DELLE VIOLAZIONI DI DATI PERSONALI

(DATA BREACH)

Documento interno – ad uso organizzativo

Versione: 1.0 **|** **Data:** 19/03/2026

Approvazione: Deliberazione del Presidente n. 51 del 19/3/2026

Gestione del documento

Versione	Data	Descrizione modifiche	Redatto/Verificato/Approvato
V 1.0	[GG/MM/AAAA]	Prima emissione (redazione completa della procedura e allegati).	[Nominativi/Firme]

Sommario

1. Premessa

La presente procedura disciplina, per la Provincia di Foggia, le attività da svolgere in caso di violazione di dati personali (di seguito "data breach"), con l'obiettivo di:

- garantire una gestione tempestiva e coordinata degli incidenti che possono coinvolgere dati personali;
- valutare in modo documentato il rischio per i diritti e le libertà delle persone fisiche;
- assicurare, ove necessario, la notifica all'Autorità Garante e/o la comunicazione agli interessati nei termini previsti dal GDPR;
- documentare le violazioni e le decisioni assunte, in attuazione del principio di responsabilizzazione (accountability).

La procedura è coerente con il Regolamento (UE) 2016/679 (in particolare artt. 4, 32, 33 e 34) e con le linee guida e provvedimenti di riferimento indicati nella sezione 4.

La procedura si applica a tutte le unità organizzative dell'Ente e a chiunque operi sotto l'autorità dell'Ente (dipendenti, collaboratori, tirocinanti, volontari, ecc.) e ai responsabili del trattamento (fornitori) che trattano dati personali per conto dell'Ente (cfr. art. 33, par. 2 GDPR e clausole contrattuali ex art. 28 GDPR).

Per incidenti di sicurezza che non comportano un coinvolgimento di dati personali (es. guasti tecnici senza impatto su dati), si applicano le procedure ICT/cybersecurity interne; qualora emerga anche solo il sospetto di coinvolgimento di dati personali, si applica la presente procedura.

2. Definizione di una violazione dei dati personali

Ai sensi dell'art. 4, punto 12 del GDPR, per "violazione dei dati personali" si intende una violazione di sicurezza che comporta, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso a dati personali trasmessi, conservati o comunque trattati.

La natura della violazione può essere ricondotta, anche ai fini della valutazione del rischio e della notifica, ai seguenti principi di sicurezza delle informazioni (cfr. provv. Garante n. 157/2019; WP29 WP250 rev.01):

- violazione della riservatezza (confidentiality breach): divulgazione o accesso non autorizzato/accidentale;
- violazione dell'integrità (integrity breach): modifica non autorizzata/accidentale dei dati personali;
- violazione della disponibilità (availability breach): perdita, distruzione o indisponibilità non autorizzata/accidentale dei dati personali.

Esempi ricorrenti (non esaustivi) di eventi che possono integrare un data breach:

- furto o smarrimento di dispositivi/documenti contenenti dati personali (PC, smartphone, supporti rimovibili, fascicoli cartacei);

- invio di comunicazioni contenenti dati personali a destinatari errati (e-mail, PEC, posta ordinaria);
- accesso abusivo a sistemi o account (es. credenziali compromesse, phishing, credential stuffing);
- malware e ransomware che compromettono la disponibilità e/o la riservatezza dei dati;
- pubblicazione accidentale online di dati personali (es. file in aree web non protette, errate impostazioni di condivisione).

Un incidente ICT non costituisce necessariamente un data breach. È data breach quando l'incidente riguarda dati personali e determina (o può determinare) uno degli impatti sopra indicati (riservatezza, integrità, disponibilità).

Tempo zero (T0). Ai fini del rispetto del termine di 72 ore per la notifica all'Autorità (art. 33, par. 1 GDPR), l'Ente considera "T0" il momento in cui il Titolare (o il soggetto formalmente delegato alla gestione dell'evento) viene a conoscenza della violazione in modo sufficientemente fondato, ossia quando dispone di un livello ragionevole di certezza che si è verificata una violazione di dati personali (concetto di "awareness" richiamato nelle linee guida WP250/EDPB).

3. Ruoli e responsabilità

La gestione di un data breach richiede il coinvolgimento coordinato di più funzioni. Coerentemente con l'assetto organizzativo dell'Ente, e con gli accordi contrattuali con i responsabili del trattamento, si riportano i ruoli e le responsabilità di ciascuna figura coinvolta nel processo di gestione e segnalazione delle violazioni.

Ruolo	**Responsabilità principali**
Titolare del trattamento (Ente / Legale rappresentante)	Assicura l'adozione della presente procedura; decide e autorizza la notifica al Garante e la comunicazione agli interessati; garantisce risorse e misure tecniche/organizzative adeguate (artt. 24 e 32 GDPR).
Segreteria generale dell'Ente	Coordina il processo e l'escalation; convoca il gruppo di gestione; assicura la tracciabilità delle decisioni; cura i rapporti interni tra strutture organizzative.
RPD/DPO (Responsabile della Protezione dei Dati)	Supporta l'analisi e la valutazione del rischio; fornisce pareri su notifica/comunicazione; supporta la conformità agli artt. 33-34 GDPR e alle linee guida; mantiene i contatti con l'Autorità ove previsto (art. 39 GDPR).

Servizio Sistemi Informativi (SSI)	Raccoglie e consolida le informazioni; compila/aggiorna la scheda evento (Allegato A) e il registro (Allegato C); predispone la notifica e le comunicazioni. Esegue contenimento, analisi tecnica, ripristino e raccolta evidenze; valuta impatti su sistemi e dati; propone misure correttive/preventive (art. 32 GDPR).
Amministratori di Sistema / Gestori piattaforme	Monitorano gli eventi di sicurezza; forniscono log/evidenze; attuano misure tecniche urgenti (es. disabilitazione account, patch).
Responsabili di servizio / Proprietari del processo (titolari del procedimento)	Segnalano tempestivamente eventi e collaborano al reperimento delle informazioni (categorie dati, finalità, interessati, misure in essere).
Ufficio legale	Supporta la valutazione di profili contrattuali e responsabilità; supporta comunicazioni formali e rapporti con terzi.
Ufficio comunicazione	Gestisce le comunicazioni esterne e agli interessati; predispone testi chiari e coerenti; coordina eventuale comunicazione pubblica.
Responsabili del trattamento (fornitori)	Informano l'Ente senza ingiustificato ritardo quando vengono a conoscenza di una violazione (art. 33, par. 2 GDPR); collaborano fornendo informazioni/evidenze e attuano le misure richieste dal Titolare (art. 28 GDPR).
Personale autorizzato al trattamento / dipendenti	Segnalano immediatamente sospetti o evidenze di violazioni; adottano comportamenti prudenziali per limitare i danni (es. non inoltrare dati, non cancellare evidenze).

Gruppo di gestione del Data Breach (GdDB). Per garantire tempestività, l'Ente istituisce (o individua) un gruppo di gestione composto almeno da: funzione di coordinamento (Segretario Generale), RPD/DPO, SSI, responsabile del servizio coinvolto. Il gruppo opera secondo le fasi della sezione 5.

4. Riferimenti

Riferimenti normativi e linee guida esterne:

- Regolamento (UE) 2016/679 (GDPR) – testo ufficiale su EUR-Lex
- D.Lgs. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali) – testo vigente su Normattiva
- D.Lgs. 10 agosto 2018, n. 101 (disposizioni di adeguamento nazionale al GDPR) – testo su Normattiva

- WP29 – Linee guida sulla notifica dei data breach (WP 250 rev.01) – pagina European Commission Newsroom
- Garante Privacy – Provvedimento n. 157 del 30 luglio 2019 (docweb 9126951)
- Garante Privacy – Provvedimento n. 209 del 27 maggio 2021 (docweb 9667201)
- EDPB – Guidelines 01/2021 (Examples) on personal data breach notification
- EDPB – Guidelines 9/2022 (Version 2.0) on personal data breach notification under GDPR
- Garante – Servizi online: Notifica data breach (istruzioni procedura telematica)
- Garante – Tool di autovalutazione (self-assessment)

5. Procedura di data breach

La procedura è articolata nelle seguenti fasi, da attivare anche in presenza di un semplice sospetto di violazione. La compilazione della scheda evento (Allegato A) accompagna tutte le fasi e viene aggiornata progressivamente.

Fase	**Attività principali**	**Output/Documenti**
Fase 1 – Segnalazione/identificazione	Ricezione della segnalazione (interna o esterna) e apertura dell'evento; attivazione SSI	Allegato A (sezione iniziale)
Fase 2 – Triage e contenimento	Contenimento tecnico/organizzativo immediato per limitare la diffusione o ulteriori impatti; preservazione evidenze.	Log, snapshot, ticket ICT
Fase 3 – Riscontri interni	Accertamento se l'evento costituisce un data breach; raccolta informazioni minime (dati, interessati, sistemi, misure). Definizione del T0.	Allegato A (aggiornato)
Fase 4 – Valutazione rischio e mitigazione	Valutazione del rischio (rischio / rischio elevato / improbabile) e definizione misure mitigative. Parere DPO.	Verbale decisione; Allegato A
Fase 5 – Notifica/comunicazione	Se dovute: notifica al Garante entro 72 ore dal T0 (art. 33 GDPR) e/o comunicazione agli interessati senza ingiustificato ritardo (art. 34 GDPR).	Ricevuta notifica; Allegato B
Fase 6 – Chiusura, registro e piano di rimedio	Aggiornamento del registro (art. 33, par. 5 GDPR) e definizione piano di rimedio/miglioramento (art. 32 GDPR).	Allegato C; piano azioni

Tempistiche. Il GDPR impone la notifica al Garante "senza ingiustificato ritardo e, ove possibile, entro 72 ore" dal momento in cui il Titolare è venuto a conoscenza della violazione (art. 33, par. 1 GDPR). Per rispettare tale vincolo, l'Ente definisce tempistiche interne (SLA) e canali di escalation; tali SLA hanno natura organizzativa e possono essere adattati in base a complessità e disponibilità delle informazioni.

- Segnalazione interna (personale/fornitori) al canale dedicato: immediata, comunque entro poche ore dalla rilevazione/sospetto.
- Attivazione triage e contenimento: il prima possibile, preferibilmente entro la stessa giornata.
- Valutazione preliminare e raccolta informazioni minime per decisione: entro 24 ore dal ricevimento della segnalazione, se possibile.
- Decisione su notifica/comunicazione: il prima possibile e comunque in tempo utile per rispettare le 72 ore dal T0 (art. 33 GDPR).

Nota: la notifica può essere trasmessa per fasi qualora non tutte le informazioni siano disponibili contestualmente (art. 33, par. 4 GDPR; WP250/EDPB). In tal caso, l'Ente invia una prima notifica con le informazioni disponibili e segue con integrazioni successive non appena possibile.

6. Identificazione di un potenziale data breach

Un potenziale data breach può essere rilevato da fonti interne o esterne. A titolo esemplificativo:

- sistemi di monitoraggio e sicurezza ICT (SIEM, antivirus/EDR, log server, alert cloud, ecc.);
- personale dell'Ente e soggetti autorizzati al trattamento;
- responsabili del trattamento e sub-responsabili (fornitori);
- cittadini/interessati; segnalazioni URP;
- altre autorità, organismi di vigilanza o media.

Obbligo di segnalazione interna. Chiunque (personale o collaboratori) venga a conoscenza o sospetti una violazione di dati personali deve effettuare una segnalazione immediata:

- al SSI: [segnalazioni.incidenti@provincia.foggia.it];
- al RPD/DPO: [Rete Entionline All Privacy – consulenza@entionline.it].
- compilando, ove possibile, il Modello interno di segnalazione (Allegato A) o fornendo le informazioni minime richieste.

Indicazioni operative per chi segnala:

- non cancellare e-mail, file o log collegati all'evento; preservare eventuali prove;
- se l'evento riguarda un invio errato, contattare immediatamente il destinatario chiedendo la cancellazione/distruzione e conferma scritta;
- se l'evento riguarda credenziali, cambiare password e avvisare ICT per blocco/rotazione credenziali;

- se l'evento riguarda dispositivi smarriti/furto, effettuare denuncia secondo le procedure interne e informare il SSI per eventuale wipe remoto.

Apertura dell'evento. Il SSI assegna un codice identificativo univoco alla segnalazione e avvia l'aggiornamento della scheda evento (Allegato A).

7. Esecuzione dei riscontri interni

Ricevuta la segnalazione, il Gruppo di gestione del Data Breach (GdDB) effettua i riscontri iniziali per:

- confermare se sono coinvolti dati personali e se l'evento rientra nella definizione di data breach (art. 4, punto 12 GDPR);
- delimitare l'ambito dell'evento (sistemi/servizi/processi coinvolti);
- stabilire il "T0" (momento di conoscenza della violazione ai fini del termine di 72 ore – art. 33 GDPR);
- raccogliere le informazioni minime necessarie a valutare il rischio e decidere sulla notifica/comunicazione.

Informazioni minime da raccogliere (da aggiornare in Allegato A):

- data e ora dell'evento (se nota o presunta) e data/ora della scoperta;
- tipo di violazione (riservatezza/integrità/disponibilità) e causa probabile;
- categorie di dati coinvolti (es. identificativi, contatti, dati particolari ex art. 9 GDPR, dati giudiziari ex art. 10 GDPR);
- categorie e stima del numero di interessati coinvolti;
- contesto: finalità del trattamento e possibili conseguenze per gli interessati;
- misure di sicurezza in essere (es. cifratura, backup, controllo accessi, logging) e loro efficacia;
- azioni di contenimento già adottate e ulteriori azioni necessarie;
- coinvolgimento di responsabili del trattamento/fornitori e informazioni disponibili da parte loro (art. 33, par. 2 GDPR).

Preservazione delle evidenze. Il SSI assicura la conservazione delle evidenze tecniche utili (log, copie forensi, ticket, screenshot, report EDR/antivirus, ecc.) compatibilmente con le regole di sicurezza e con eventuali esigenze investigative.

Nel caso in cui la violazione coinvolga un responsabile del trattamento, il SSI richiede formalmente al fornitore tutte le informazioni necessarie (tempistiche, dati coinvolti, misure adottate, evidenze) e ne sollecita l'aggiornamento periodico fino a chiusura dell'evento (art. 28 e art. 33, par. 2 GDPR; WP250/EDPB).

8. Valutazione e mitigazione

Il Titolare valuta se la violazione possa comportare un rischio per i diritti e le libertà delle persone fisiche (art. 33 GDPR) e, se del caso, un rischio elevato (art. 34 GDPR). La valutazione deve considerare sia la gravità delle possibili conseguenze sia la probabilità che esse si verifichino (cfr. WP250 rev.01; EDPB Guidelines 9/2022).

Fattori da considerare nella valutazione (indicazioni WP250/EDPB):

- tipologia di violazione (riservatezza/integrità/disponibilità) e durata dell'esposizione/indisponibilità;
- natura, sensibilità e volume dei dati (inclusa presenza di categorie particolari di dati ex art. 9 GDPR o dati ex art. 10 GDPR);
- facilità di identificazione degli interessati e possibilità di riutilizzo illecito dei dati (es. credenziali, documenti, IBAN);
- numero di interessati coinvolti e ampiezza geografica/organizzativa dell'impatto;
- caratteristiche degli interessati (es. soggetti vulnerabili) e del contesto del trattamento (es. servizi sociali, minori);
- caratteristiche del destinatario/attaccante (es. destinatario "affidabile" in caso di invio errato vs soggetto ignoto);
- misure di protezione in essere e loro efficacia (es. cifratura robusta, hashing con salt, backup, pseudonimizzazione).

Supporto operativo. Il GdDB può utilizzare, come ausilio alla valutazione, il tool di autovalutazione del Garante (https://servizi.gpdp.it/databreach/s/self-assessment), ferma restando la necessità di una valutazione specifica e documentata per il caso concreto.

Esito della valutazione e decisioni:

- Rischio improbabile: non è dovuta la notifica al Garante; resta obbligatoria la documentazione nel registro (art. 33, par. 5 GDPR).
- Rischio: è dovuta la notifica al Garante (art. 33 GDPR).
- Rischio elevato: oltre alla notifica al Garante, è dovuta la comunicazione agli interessati (art. 34 GDPR), salvo eccezioni.

Mitigazione. Parallelamente alla valutazione, il SSI e le strutture coinvolte adottano misure tecniche e organizzative per contenere e ridurre gli impatti, ad esempio:

- isolamento dei sistemi coinvolti e blocco degli accessi non autorizzati;
- reset/rotazione credenziali e revoca token di accesso;
- ripristino da backup e verifica integrità dei dati;
- patching di vulnerabilità e hardening configurazioni;
- recupero/cancellazione dati inviati erroneamente, richiesta di conferma di cancellazione;
- monitoraggio rafforzato e attivazione misure antifrode, se pertinenti.

Le misure adottate e quelle pianificate devono essere descritte nella scheda evento (Allegato A) e, ove necessario, riportate nella notifica al Garante e/o nella comunicazione agli interessati (artt. 33, par. 3 e 34, par. 2 GDPR).

9. Notifica all'Autorità Garante

Quando la violazione è suscettibile di presentare un rischio per i diritti e le libertà delle persone fisiche, il Titolare notifica la violazione all'Autorità Garante per la protezione dei dati personali senza ingiustificato ritardo e, ove possibile, entro 72 ore dal T0 (art. 33, par. 1 GDPR).

La notifica avviene tramite procedura telematica nel portale dei servizi online del Garante, raggiungibile all'indirizzo https://servizi.gpdp.it/databreach/s/ , secondo il provvedimento n. 209/2021 e le istruzioni operative pubblicate dal Garante.

Contenuti minimi della notifica (art. 33, par. 3 GDPR):

- descrizione della natura della violazione (inclusi, ove possibile, categorie e numero approssimativo di interessati e di registrazioni di dati);
- nome e dati di contatto del RPD/DPO o di altro punto di contatto;
- descrizione delle probabili conseguenze della violazione;
- descrizione delle misure adottate o proposte per porre rimedio alla violazione e attenuarne gli effetti negativi.

Notifica per fasi. Se non è possibile fornire tutte le informazioni contestualmente, la notifica può essere effettuata in più fasi senza ulteriore ingiustificato ritardo (art. 33, par. 4 GDPR; WP250/EDPB).

Ritardo. Se la notifica avviene oltre le 72 ore, il Titolare deve indicare i motivi del ritardo (art. 33, par. 1 GDPR; WP250).

Flusso interno di approvazione (modello suggerito):

- Il SSI e l'unità organizzativa/struttura competente compilano le informazioni tecniche e di contesto nella scheda evento (Allegato A).
- Il RPD/DPO supporta la valutazione e formula un parere (non vincolante) su notifica/comunicazione, da allegare o richiamare.
- La Segreteria Generale dell'Ente sottopone la bozza di notifica al Segretario Generale per approvazione.
- L'invio avviene tramite portale telematico; la ricevuta/protocollo vengono conservati e registrati (Allegato C).

Aggiornamenti/integrazioni successive. Qualora emergano ulteriori informazioni dopo la notifica, l'Ente effettua comunicazioni integrative al Garante tramite la medesima procedura telematica, aggiornando la scheda evento e il registro delle violazioni.

10. Comunicazione agli interessati

Quando la violazione è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare comunica la violazione agli interessati senza ingiustificato ritardo (art. 34, par. 1 GDPR). La comunicazione deve essere redatta in linguaggio chiaro e semplice.

Contenuti minimi della comunicazione (art. 33, par. 3, lettere b), c) e d), GDPR):

- descrizione della natura della violazione;
- nome e dati di contatto del RPD/DPO o di altro punto di contatto;
- descrizione delle probabili conseguenze della violazione;
- descrizione delle misure adottate o proposte per porre rimedio alla violazione e attenuarne gli effetti negativi, incluse eventuali raccomandazioni pratiche agli interessati.

La comunicazione è predisposta con il supporto del RPD/DPO e dell'Ufficio comunicazione; l'Ufficio legale può essere coinvolto per la revisione. Si utilizza il modello di cui all'Allegato B, adattandolo al caso concreto.

Canali di comunicazione (da scegliere in base a efficacia e proporzionalità):

- comunicazione individuale (e-mail, PEC, lettera) quando possibile;
- avviso sul sito istituzionale e/o comunicazione pubblica equivalente quando la comunicazione individuale richiede sforzi sproporzionati (art. 34, par. 3, lett. c GDPR);
- altri canali idonei (es. area riservata, messaggi in app) se disponibili e tracciabili.

Casi in cui la comunicazione agli interessati può non essere necessaria (art. 34, par. 3 GDPR):

- sono state applicate misure tecniche/organizzative adeguate che rendono i dati incomprensibili a chiunque non sia autorizzato (es. cifratura efficace);
- sono state adottate successivamente misure che scongiurano il rischio elevato per gli interessati;
- richiede sforzi sproporzionati: in tal caso si procede con comunicazione pubblica o misura simile, con analoga efficacia.

Qualora si decida di non comunicare agli interessati, le motivazioni devono essere documentate nella scheda evento e nel registro (art. 33, par. 5 GDPR; WP250). L'Autorità di controllo può comunque richiedere che sia effettuata la comunicazione.

11. Aggiornamento del registro delle violazioni

Indipendentemente dall'obbligo di notifica, il Titolare documenta qualsiasi violazione dei dati personali, incluse le circostanze, le conseguenze e i provvedimenti adottati per porvi rimedio (art. 33, par. 5 GDPR). La documentazione deve consentire all'Autorità di verificare il rispetto degli obblighi di cui all'art. 33.

Il registro delle violazioni è tenuto dal SSI, con il supporto delle unità organizzative/strutture coinvolte. La scheda evento (Allegato A) alimenta il registro (Allegato C).

Conservazione. Il registro e le evidenze collegate (ticket, log, ricevute, bozze comunicazioni) sono conservati secondo le regole di gestione documentale dell'Ente e resi disponibili, su richiesta, all'Autorità competente.

12. Definizione del piano di rimedio

A seguito della gestione del data breach, il Titolare, con il supporto del RPD/DPO e di ICT/Sicurezza, effettua una revisione post-incidente (post-mortem) finalizzata a:

- analizzare le cause (tecniche, organizzative, errore umano, fornitore) che hanno determinato la violazione;
- valutare l'efficacia delle misure tecniche e organizzative adottate (art. 32 GDPR) e delle misure di contenimento/risposta;
- identificare azioni correttive e preventive (hardening, procedure, formazione, controlli, audit su fornitori);
- aggiornare, se necessario, valutazioni d'impatto (DPIA) e registro dei trattamenti (art. 30 GDPR) per processi interessati;
- verificare e, se necessario, migliorare le clausole contrattuali/SLA con i responsabili del trattamento (art. 28 GDPR).

Il piano di rimedio indica responsabilità, scadenze e modalità di verifica dell'attuazione. Le azioni e la loro chiusura devono essere tracciate (es. ticketing o verbali) e richiamate nel registro delle violazioni.

Formazione e consapevolezza. In coerenza con il principio di responsabilizzazione (art. 5, par. 2 GDPR) e con le indicazioni delle linee guida WP250, l'Ente promuove attività periodiche di informazione/formazione affinché il personale sappia riconoscere e segnalare tempestivamente potenziali violazioni.

Allegato A – Modello interno di segnalazione di un data breach (Scheda evento)

Compilare quanto disponibile al momento della segnalazione. La scheda viene aggiornata progressivamente durante la gestione dell'evento.

Campo	**Valore / Note**
Codice evento/violazione	
Struttura/servizio coinvolto	
Segnalatore (nome, ruolo, contatti)	
Data e ora della segnalazione	
Data e ora dell'evento (nota o presunta)	
Data e ora della scoperta	
Modalità di scoperta/segnalazione (es. alert, cittadino, fornitore)	
Descrizione sintetica dell'evento	
Tipologia (riservatezza / integrità / disponibilità)	
Sistemi/servizi coinvolti (applicazioni, server, archivi cartacei, ecc.)	
Categorie di dati personali coinvolti	
Presenza di categorie particolari di dati (art. 9 GDPR) o dati ex art. 10 GDPR	
Categorie di interessati coinvolti	
Numero approssimativo di interessati	
Numero approssimativo di record/dati coinvolti	
Misure di sicurezza in essere (es. cifratura, backup, access control)	
Azioni immediate intraprese (contenimento/mitigazione)	
Responsabili del trattamento/fornitori coinvolti (se applicabile)	
Valutazione preliminare del rischio (improbabile / rischio / rischio elevato) e motivazioni	
Data e ora T0 (awareness)	
Parere RPD/DPO (data e sintesi)	
Decisione Titolare su notifica al Garante (sì/no) + motivazione	
Data/ora notifica al Garante e riferimento ricevuta/protocollo	
Decisione su comunicazione agli interessati (sì/no) + motivazione	
Canali e data/ora comunicazione agli interessati	
Ulteriori comunicazioni/adempimenti (altri enti/autorità) – se applicabile	
Note e chiusura evento (data chiusura, lessons learned, azioni di rimedio)	

Allegato B – Modello comunicazione agli interessati (art. 34 GDPR)

Oggetto: Comunicazione di violazione di dati personali ai sensi dell'art. 34 del Regolamento (UE) 2016/679

Gentile [Nome/Cognome],

la informiamo che in data [GG/MM/AAAA] la Provincia di Foggia ha rilevato una violazione di dati personali che potrebbe riguardare i Suoi dati.

1) Natura della violazione (art. 34, par. 2, lett. a GDPR)

[Descrivere in modo chiaro e semplice cosa è accaduto, quando e quali sistemi/processi sono coinvolti.]

2) Dati di contatto (art. 34, par. 2, lett. b GDPR)

RPD/DPO: [Nome e Cognome] – [e-mail] – [telefono] – [PEC (se disponibile)].

3) Possibili conseguenze (art. 34, par. 2, lett. c GDPR)

[Descrivere le probabili conseguenze per l'interessato: es. rischio di phishing, accessi non autorizzati, indisponibilità temporanea, ecc.]

4) Misure adottate o proposte (art. 34, par. 2, lett. d GDPR)

[Descrivere le misure adottate dall'Ente (contenimento, ripristino, blocco credenziali, ecc.) e quelle pianificate.]

5) Raccomandazioni pratiche per l'interessato (se del caso)

[Esempi: cambiare password, attenzione a e-mail sospette, monitorare movimenti bancari, ecc. – adattare al caso concreto.]

L'Ente resta a disposizione per qualsiasi chiarimento tramite i contatti sopra indicati.

Cordiali saluti,

[Firma del Titolare o soggetto delegato]

[Ruolo]

Provincia di Foggia

Allegato C – Registro delle violazioni (art. 33, par. 5 GDPR)

Il registro documenta tutte le violazioni (notificate e non notificate) e le relative decisioni. Per ciascun evento devono essere conservate, ove disponibili, le evidenze tecniche e documentali (ticket, log, ricevute, ecc.).

Codice	**Data evento/scoperta/T0**	**Natura e causa (C/I/A)**	**Dati e interessati coinvolti**	**Valutazione rischio (motivazione)**	**Adempimenti (Garante/Interessati/Altro)**	**Misure adottate/proposte**	**Chiusura e note**