

Gentile Utente

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

Gentile Utente,

La informiamo che, a seguito di alcune verifiche informatiche, abbiamo rilevato un incidente di sicurezza (*data breach*) avvenuto in data 28.08.2026, causato da soggetti esterni non identificati. Questo evento ha determinato un accesso non autorizzato ad alcuni dati personali presenti nei nostri sistemi e relativi alle utenze del servizio idrico.

Per individuare con precisione i soggetti e le informazioni potenzialmente coinvolti è stato necessario svolgere approfondite analisi tecniche e di sicurezza da parte delle nostre strutture IT che hanno richiesto il tempo tecnico indispensabile per ricostruire nel dettaglio le dinamiche dell'evento e circoscrivere gli accessi impropri. Le verifiche tecniche sono ancora in corso e non ancora siamo in grado di identificare con esattezza tutte le utenze interessate, ma riteniamo necessario e opportuno – al fine di garantire la sicurezza dei nostri utenti – trasmettere in allegato alla prima fatturazione utile e pubblicare sul sito istituzionale, anche in via precauzionale, questa comunicazione, come previsto dall'art. 34 del Regolamento (UE) 2016/679 e in conformità con le Linee guida EDPB n. 9/2022.

Di seguito Le forniamo, quindi, tutte le informazioni utili relative all'evento e alle misure adottate.

1. Natura della violazione e dati coinvolti

Da informazioni assunte risulta che l'attacco informatico ha comportato l'accesso non autorizzato e la momentanea perdita di disponibilità di dati personali correlati all'emissione delle bollette.

I dati potenzialmente impattati includono:

Dati anagrafici e identificativi: nome, cognome e codice fiscale dell'intestatario dell'utenza;

Indirizzo della fornitura: ubicazione e dati dell'utenza idrica;

Dati di contatto: indirizzo e-mail e numero di telefono;

Dati tecnici dell'utenza: numero di matricola del contatore.

Nota importante sui Dati Particolari (Art. 9 GDPR): Si precisa che, per quanto a conoscenza, gli archivi violati non contenevano dati rientranti nelle categorie particolari di cui all'art. 9 del Regolamento UE 2016/679, in quanto tali informazioni non erano presenti sui sistemi oggetto

dell'attacco ma in altri (archivio cartaceo, medico competente, altre applicazioni non violate). Anche i documenti di identità acquisiti per finalità connesse agli allacci idrici non sono stati violati.

2. Possibili conseguenze per gli interessati

La violazione dei dati in potrebbe comportare i seguenti rischi:

- Tentativi di truffa, *phishing* o *smishing* via e-mail, telefono, whatsapp o SMS mediante l'uso di comunicazioni ingannevoli che sfruttano i dati anagrafici o l'appartenenza all'Azienda;
- Tentativi di accesso non autorizzato a servizi personali tramite tecniche di ingegneria sociale (comunicazioni fraudolente o tentativi di contatto ingannevoli)

3. Misure di attenuazione e azioni intraprese dall'Azienda

L'Azienda ha reagito tempestivamente mettendo in atto le seguenti misure di sicurezza e salvaguardia:

- Isolamento e messa in sicurezza immediata dei sistemi informatici coinvolti per arrestare l'accesso non autorizzato;
- Ripristino dei servizi mediante procedure di raccomandata sicurezza e backup verificate;
- Rafforzamento delle misure di sicurezza;
- Notifica ad ACN (Agenzia Cybersicurezza Nazionale)
- Notifica formale dell'incidente all'Autorità Garante per la protezione dei dati personali ai sensi dell'art. 33 del GDPR;
- Denuncia dell'accaduto alle Autorità di Polizia Giudiziaria preposte (Polizia Postale).

4. Raccomandazioni e consigli utili

Al fine di prevenire e mitigare eventuali rischi individuali, Le suggeriamo di adottare le seguenti precauzioni:

1. **Prestare massima attenzione alle comunicazioni in arrivo:** Diffidare di e-mail, PEC, SMS, messaggi Whatsapp o telefonate sospette che richiedano la condivisione di credenziali, codici di accesso, conferme di dati bancari o il pagamento di somme di denaro. Infatti, considerata la tipologia di dati coinvolti, potrebbe esserci il rischio che Lei riceva comunicazioni fraudolente o tentativi di contatto ingannevoli che fanno riferimento alla sua utenza. Per questo Le consigliamo di prestare particolare attenzione a eventuali messaggi sospetti, soprattutto se richiedono dati personali o finanziari o contengono link o allegati inattesi. In caso di dubbio, verifichi sempre l'affidabilità del mittente.
2. **Non aprire allegati o link sospetti:** Evitare di cliccare su collegamenti ipertestuali contenuti in e-mail, PEC, SMS, messaggi whatsapp da mittenti sconosciuti o con contenuti anomali.

Le ricordiamo inoltre che ACA S.p.A. non la contatterà mai per chiederLe password o dati di pagamento

5. Contatti del Responsabile della Protezione dei Dati (DPO)

Per qualsiasi chiarimento, informazione aggiuntiva o per segnalare anomalie correlate a questa comunicazione, è possibile contattare il Responsabile della Protezione dei Dati (DPO/RPD) dell'Azienda al seguente recapito e-mail: **dpo@aca.pescara.it**

La sicurezza dei Suoi dati costituisce una priorità assoluta per questa Azienda e ci impegniamo a fornirLe eventuali ulteriori aggiornamenti qualora dovessero emergere nuovi elementi rilevanti.

Sarà cura di ACA S.p.A. provvedere ad effettuare comunicazioni agli interessati qualora all'esito delle indagini in corso dovesse emergere la violazione, al momento non nota, di ulteriori categorie di dati personali.

Distinti saluti.

Il Direttore Generale ACA S.p.A.
Dott. Marco Santedicola



Signed with  NamirialSign

MARCO SANTEDICOLA
09/10/2026 10:25:56 UTC+0200