COMUNICAZIONE DI VIOLAZIONE DI DATI PERSONALI

Sassuolo, 27 Agosto 2026

A tutti i nostri Clienti e Fornitori.

Siamo con la presente a rendere noto che un Responsabile esterno del Trattamento di **Solution Care Srl** è stato recentemente oggetto di un attacco informatico accidentale e imprevedibile, condotto da parte di un gruppo di hacker, che ha comportato la violazione di dati personali (c.d. Data Breach).

> ***Nota:*** *Si precisa che, alla data del 24/08/2026, si sono concluse con esito positivo le operazioni di ripristino dell'intera infrastruttura IT del Responsabile del Trattamento, mediante procedure di restore dei dati da copie di backup conservate su sistemi Cloud protetti e segregati, consentendo la piena ripresa delle attività operative. Le operazioni di remediation e ripristino si sono svolte in modalità graduale e controllata, con preminente priorità alla messa in sicurezza delle banche dati e alla verifica dell'assenza di codice malevolo residuo idoneo a re-infettare nuovamente i loro sistemi.*

Cosa è accaduto

Nell'ambito delle ordinarie e continue attività di monitoraggio e controllo della infrastuttura IT, presso un nostro **Responsabile esterno del Trattamento** debitamente nominato ai sensi dell'Art. 28 del GDPR, è stato rilevato un incidente di sicurezza che ha interessato alcuni sistemi di archiviazione (Server di rete e NAS) e applicativi gestionali (CRM) ed altri Servizi gestiti presso il loro Data Center. Nei suddetti sistemi sono conservati dati personali di cui **Solution Care Srl** è Titolare e che ci sono stati conferiti nel tempo dagli interessati in virtù dei rapporti commerciali in essere ovvero acquisiti in forza di altri presupposti di liceità.

L'evento lesivo ci è stato comunicato dal Responsabile nel pomeriggio del **17/08/2026**. La violazione è avvenuta durante il periodo di chiusura aziendale per la pausa estiva ed è stato rilevato dal Responsabile in data **14/08/2026**; sulla base dei rilievi delle prime analisi, l'attacco risulterebbe però iniziato nella tarda serata del **13/08/2026**.

Tipo di violazione

Mediante la diffusione di un software malevolo (riconducibile alla categoria dei malware di tipo Ransomware/CryptoLocker), le risorse informatiche ed alcuni archivi aziendali (Macchine Virtuali, DataBase, file system, ecc.) del Responsabile sono stati sottoposti a cifratura non autorizzata, rendendoli **temporaneamente indisponibili e inaccessibili.**

Natura della violazione

Mancanza di disponibilità dei dati

Sebbene allo stato attuale **non vi siano evidenze confermate di esfiltrazione**, la tipologia di incidente verificatosi potrebbe teoricamente aver esposto i dati conservati nei sistemi coinvolti a una

potenziale violazione della riservatezza (Confidentiality breach). Sono tutt'ora in corso approfondite e rigorose verifiche tecniche e di analisi da parte del Responsabile volte a fare piena luce sulla dinamica della violazione.

Causa della violazione

Azione intenzionale ed illecita perpetrata da soggetti terzi esterni (cybercriminali), corredata da richiesta di riscatto (extortion request).

Quali dati sono stati coinvolti

In base agli accertamenti e alle verifiche tecniche finora espletate, le categorie di dati personali potenzialmente interessate dalla violazione comprendono:

- Dati identificativi e anagrafici (es. nome, cognome, codice fiscale, partita IVA, codice cliente/fornitore);
- Dati di contatto (es. indirizzo di residenza/sede, indirizzo di posta elettronica ordinaria e/o PEC, numeri di telefonia fissa e/o mobile);
- Dati finanziari e di pagamento (es. coordinate bancarie IBAN, storico delle transazioni commerciali e finanziarie);
- Dati personali contenuti nei Curricula Vitae pervenuti alla Società.

Quali sono i possibili rischi per gli interessati

Qualora le indagini in corso dovessero accertare un'effettiva compromissione della riservatezza dei dati, gli interessati potrebbero essere esposti a potenziali condotte illecite o tentativi di frode da parte di terzi, quali ad esempio:

- Tentativi di Phishing tramite l'invio di e-mail ingannevoli;
- Tentativi di Smishing a mezzo SMS o servizi di messaggistica istantanea;
- Tentativi di Vishing mediante contatti telefonici fraudolenti;
- Utilizzo indebito dei dati personali per finalità di sostituzione di persona, usurpazione dell'identità o ulteriori attività illecite.

Si precisa che dalle analisi condotte sul Dark Web e nei canali informatici di monitoraggio, non si riscontrano allo stato attuale evidenze relative alla pubblicazione, divulgazione o all'utilizzo fraudolento dei dati oggetto del presente incidente.

Misure adottate

All'atto della rilevazione dell'incidente, il Responsabile del Trattamento ha tempestivamente attivato il proprio Piano di Risposta agli Incidenti di Sicurezza (Incident Response). In particolare, sono state prontamente poste in essere le seguenti azioni:

- Isolamento e contenimento tempestivo dell'incidente per impedire la propagazione del malware;
- Individuazione e neutralizzazione del vettore di attacco e della vulnerabilità sfruttata;
- Innalzamento e rafforzamento delle misure di sicurezza tecniche, cibernetiche ed organizzative a protezione degli asset aziendali;

- Esecuzione di approfondite analisi forensi tecniche e continuo monitoraggio della rete e dei sistemi;
- Adempimento formale degli obblighi normativi previsti in materia di data protection, ivi compresa la prescritta notifica all'Autorità Garante per la Protezione dei Dati Personali ai sensi dell'Art. 33 del GDPR;

Cosa possono fare gli utenti

In situazioni di questa natura, le condotte fraudolente perseguono tipicamente lo scopo di sfruttare indebitamente le informazioni personali per finalità estorsive o per l'esfiltrazione di ulteriori dati sensibili/credenziali, mediante l'invio di comunicazioni ingannevoli o l'effettuazione di chiamate a nome di operatori commerciali, ovvero mediante tentativi di intrusione negli account personali degli interessati.

Pertanto, **Solution Care Srl** invita gli interessati ad adottare le opportune cautele a tutela della propria sfera personale, raccomandando di prestare un livello di attenzione e vigilanza superiore all'ordinario nei confronti di qualsiasi interazione anomala o sospetta, sia in ambiente **digitale** che **analogico**.

A tal fine, si raccomanda di prendere visione delle schede informative di approfondimento predisposte dall'Autorità Garante per la Protezione dei Dati Personali:

- **Phishing:**
  https://www.garanteprivacy.it/temi/cybersecurity/phishing
- **Vishing:**
  https://www.garanteprivacy.it/temi/cybersecurity/vishing
- **Smishing:**
  https://www.garanteprivacy.it/temi/cybersecurity/smishing
- **smisSIM Swapping (o SIM Swap Fraud):**
  https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9572143

In questa fase, Solution Care Srl suggerisce altresì di attenersi alle seguenti buone prassi di sicurezza:

- Verificare rigorosamente l'attendibilità di qualsiasi e-mail, SMS, messaggio o chiamata telefonica con cui vengano richiesti codici di accesso, credenziali o dati personali riservati; si ricorda che gli Istituti di Credito e i fornitori di servizi primari non richiedono mai la comunicazione di password o credenziali d'accesso tramite messaggistica o telefono;
- Prestare la massima attenzione a e-mail, SMS o altre comunicazioni contenenti collegamenti ipertestuali (link) o allegati inusuali/sospetti, che potrebbero veicolare software malevoli o reindirizzare verso portali web contraffatti o dannosi;
- Verificare accuratamente l'autenticità dell'indirizzo del mittente prima di riscontrare comunicazioni non attese;
- Segnalare tempestivamente ai nostri canali di contatto ufficiali eventuali comunicazioni anomale o sospette ricevute a nome della nostra Società o recanti riferimento ai nostri servizi.

Informazioni e assistenza

Per qualsiasi chiarimento o richiesta di informazioni relativa al presente incidente, nonché per l'esercizio dei diritti riconosciuti dagli Articoli 15 e seguenti del GDPR, è possibile rivolgersi a:

Titolare del trattamento: Solution Care Srl
E-mail: info@solutioncare.it
Telefono : +39 0536 994129

Qualora il prosieguo delle attività di analisi ed indagine tecnica, tutt'ora in Corso presso il Data Center del Responsabile, dovesse far emergere ulteriori elementi di rilievo, la presente informativa sarà oggetto di tempestivo aggiornamento ed integrazione.

Nel rammaricarci per l'accaduto, confermiamo il primario impegno della scrivente di avvalersi solo di Responsabili esterni del trattamento selezionati che possano garantire elevati standard di sicurezza informatica, il rigoroso rispetto di procedure tecnico-organizzative e assicurare la massima tutela dei dati personali degli interessati.