

## **Comunicazione violazione di dati personali (data breach) agli interessati ex art. 34 Reg. UE n. 2016/679 (cd GDPR)**

Con la presente, il sottoscritto Titolare del Trattamento Società Servizi Territoriali S.P.A. (d'ora in poi per brevità anche solo "SST") desidera informare, ai sensi dell'articolo 34 del Regolamento (UE) 2016/679 ("GDPR"), di una violazione dei dati personali degli interessati che a vario titolo utilizzano i servizi di SST o che sono entrati in contatto con la nostra Società.

Come pubblicamente reso noto tramite avviso pubblicato in data 13 febbraio 2026 sul sito [www.sstchioggia.it](http://www.sstchioggia.it), la nostra Società ha subito un attacco informatico di tipo ransomware tra il 2 e 3 febbraio u.s., che ha comportato la cifratura di sistemi informatici contenenti, per quanto qui più interessa, dati personali degli interessati.

L'incidente ha determinato una temporanea indisponibilità dei dati. Non è stato possibile escludere con assoluta certezza che soggetti non autorizzati possano aver avuto accesso ai dati prima della cifratura; tuttavia, allo stato delle analisi effettuate, non vi sono evidenze di esfiltrazione, diffusione e/o pubblicazione di tali dati.

I dati personali potenzialmente interessati dalla violazione includono:

- dati anagrafici e di contatto;
- codice fiscale e, in alcuni casi, documenti di identità;
- in alcuni casi coordinate bancarie;

SST Chioggia nell'immediatezza del data breach, anche mediante l'intervento di una società esperta in cybersecurity, ha posto in essere misure tecniche e organizzative volte a porre rimedio alla violazione dei dati e a ridurre gli effetti negativi, tra cui, sintetizzando:

- immediata messa in sicurezza del perimetro di rete e isolamento e messa in sicurezza dei sistemi coinvolti;
- ripristino progressivo dei servizi essenziali da backup in ambiente segregato;
- attivazione di una soluzione antivirus/EDR;
- segmentazione della rete di management rispetto alla LAN ordinaria;
- rafforzamento del modello di backup;
- stabilizzazione del dominio e dei servizi, con progressiva ricostruzione dei componenti infrastrutturali compromessi secondo criteri di sicurezza rafforzati, con revisione di utenze, privilegi e policy
- dismissione o isolamento dei sistemi legacy maggiormente esposti;
- ulteriore irrobustimento del perimetro e degli accessi remoti;
- analisi forense del data breach

Il data breach è stato tempestivamente notificato all'autorità Garante per la protezione dei dati personali ai sensi del GDPR.

SST Chioggia ha proceduto anche alla presentazione di una denuncia-querela avanti all'autorità giudiziaria.

**A titolo precauzionale, Le consigliamo di:**

- prestare particolare attenzione a email, SMS, messaggistica istantanea (whatsapp, telegram ecc.) o telefonate sospette, anche se apparentemente provenienti da soggetti conosciuti;
- non fornire dati personali o bancari in risposta a comunicazioni non verificate;
- segnalare eventuali anomalie o sospetti tentativi di frode alle autorità competenti.

Nell'evidenziare che SST Chioggia dà la massima importanza alla tutela dei dati personali che tratta ed è spiacente per quanto occorso, si comunica che per ulteriori informazioni e/o chiarimenti è possibile contattare il referente aziendale titolare della gestione dei Servizi Informatici ovvero contattare il Responsabile della Protezione dei Dati Personali (DPO) – Avv. Federica Banfi – alla seguente e-mail [federica.banfi@crelex.it](mailto:federica.banfi@crelex.it)

Con i migliori saluti

  
**L'Amministratore Unico**  
dott. Vincenzo Vitapiano