# Sito web senza certificato SSL e HTTPS: multa da 15.000 euro

La sicurezza è un elemento fondamentale per ogni attività online, eppure ci sono ancora troppi siti web che non rispettano una misura di sicurezza base: il **protocollo HTTPS** (HyperText Transfer Protocol over Secure Socket Layer).

**Non usare il protocollo HTTPS**, oltre a **mettere a rischio i dati degli utenti** che si collegano al sito, può comportare anche una **violazione del GDPR**, il Regolamento generale sulla protezione dei dati (dall'ingleseGeneral Data Protection Regulation) che disciplina il modo in cui le aziende e le altre organizzazioni devono trattare i dati personali.

Ne sa qualcosa l'azienda **Servizio Idrico Integrato S.c.p.a** che è statada poco **sanzionata dal Garante** per la protezione dei dati personali per la **mancanza di un certificato SSL** sul proprio sito web, quindi per aver consentito l'accesso ai

propri servizi online senza una connessione HTTPS crittografata.

## Cos’è il protocollo HTTPS? Come mai è così importante?

**HTTPS** è l’acronimo di *Hypertext Transfer Protocol Secure* ed è un protocollo per la comunicazione sul web che **protegge l’integrità e la riservatezza dei dati** scambiati usando una comunicazione criptata.

Per implementare il protocollo HTTPS su proprio sito web è necessario installare un **certificato SSL**.

Senza un certificato SSL, infatti, il protocollo che viene utilizzato per la comunicazione fra il browser dell’utente e il sito web è l’**HTTP** che, a differenza dell’HTTPS, genera un **traffico** di dati anonimo e **non criptato** e quindi **vulnerabile agli attacchi informatici.**

Vuoi saperne di più sul funzionamento del protocollo HTTPS? Leggi l’articolo “Cos’è il protocollo HTTPS?“

Usare il protocollo HTTPS e offrire una connessione protetta è sicura è di fondamentale importanza per ogni sito web, in primo luogo per **proteggere i dati degli utenti** che navigano il sito ma anche per **migliorare la visibilità online** del sito web.

**Google**, infatti, ha apertamente dichiarato di **premiare i siti che hanno un certificato SSL** e una connessione sicura HTTPS e **Google Chrome**, il browser più utilizzato per navigare online, **segnala i siti web sprovvisti di protocollo HTTPS** come non sicuri.

## Sanzioni ai siti web senza HTTPS. Il caso

## di Servizio Idrico Integrato S.c.p.a

Oltre alla mancata garanzia di sicurezza data ai visitatori del sito web e alle problematiche relative all' indicizzazione su Google, l'assenza di una connessione HTTPS può far incorrere anche in **sanzioni amministrative per la violazione di alcuni principi sanciti dal GDPR**, il Regolamento generale sulla protezione dei dati.

È quello che è successo ultimamente al **Servizio Idrico Integrato S.c.p.a**. L'Azienda ha infatti ricevuto una sanzione di 15.000 euro dal Garante della privacy per non aver usato il protocollo HTTPS.

Su segnalazione di un utente il Garante della privacy ha accertato che l'azienda **non aveva protetto con HTTPS un'area riservata del proprio sito web**. Per l'accesso a tale area veniva richiesto l'inserimento di username e password utilizzando il protocollo HTTP non consente il criptaggio dei dati inseriti.

Servizio Idrico Integrato S.c.p.a. si è difesa specificando che all'interno dell'area riservata in questione non sono presenti dati di pagamento e che non risultano violazioni dei dati.

## Le motivazioni del Garante della privacy alla multa inflitta al Servizio Idrico Integrato

Il Garante ha ritenuto che l'assenza del protocollo HTTPS viola importanti principi sanciti dal GDPR come quello dell'**integrità e riservatezza dei dati trattati** e quello di **protezione dei dati** fin dalla progettazione.

Per rispettare il principio di **"integrità e riservatezza"** (art.5 par.1 lett.f), l'art. 32 par.1 del Regolamento prevede che il titolare del trattamento, *"tenendo*

*conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche,* ***debba mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso, "la cifratura dei dati personali"****.*

Inoltre, per il principio di "Privacy by Design", in fase di progettazione e realizzazione di un sito internet, il titolare deve (cfr. le Linee guida 4/2019 sull'articolo 25, spec. punto 85):

- valutare i rischi per la sicurezza dei dati personali, considerando l'impatto sui diritti e le libertà degli interessati, e contrastare efficacemente quelli identificati;
- proteggere i dati personali da modifiche e accessi non autorizzati e accidentali durante il loro trasferimento.

## Certificati SSL e HTTPS. Come evitare sanzioni

Per **implementare il protocollo HTTPS** ed evitare le sanzioni amministrative previste dal GDPR è necessario **installare un certificato SSL** su proprio sito web. L'uso di un certificato SSL consente infatti, grazie all'utilizzo del protocollo HTTPS, lo scambio sicuro dei dati online.

Per garantire ai tuoi utenti una connessione sicura e protetta nello scambio di dati ed evitare sanzioni scegli i certificati SSL di Register.it .

Sono emessi da SECTIGO, leader mondiale nella sicurezza del web, e si dividono in **Domain Validated** (DV), **Organization Validated** (OV) ed **Extended Validation** (EV) a seconda se conferiscono la certificazione al solo dominio o se

certificano anche l’azienda.