



I.s.e.c. Srl

Taggia, li 03 novembre 2022

Spett.le Enti

PROTOCOLLO INTERNET HTTP A RISCHIO DI CYBERATTACCHI

In merito al protocollo Internet dei siti web e accessi ai servizi on line, Vi ricordiamo che il Garante della privacy ha sanzionato, con **provvedimento del 6 ottobre 2022** (link: <https://www.garanteprivacy.it/web/quest/home/docweb/-/docweb-display/docweb/9817058>), un'Azienda fornitrice di servizi idrici per 15.000 euro, per non aver protetto adeguatamente i dati dei clienti registrati sull'area riservata del proprio sito web.

Nel caso di specie, a seguito di un reclamo l'Autorità ha accertato che l'accesso al sito web dell'Azienda dedicato ai "servizi online" avveniva tramite il protocollo di rete "http", non crittografato e non sicuro.

Il Garante ha evidenziato che l'utilizzo di un protocollo non protetto (http) rispetto al protocollo httpS (dove S sta per *secure*), non garantisce una adeguata tutela dei dati personali con il rischio concreto, ad esempio, di furti d'identità, con acquisizione di dati per utilizzi illeciti.

Il provvedimento del Garante è andato anche più nello specifico, osservando che nonostante non vi fossero state violazioni accertate, gli obblighi di adeguate misure di sicurezza andavano applicati anche ai sistemi preesistenti alla data di efficacia del Regolamento (25 maggio 2018).

Trattandosi di un alto numero di potenziali utenti coinvolti e di un'ampia categoria di dati personali raccolti (dalle credenziali di autenticazione (nome utente e password) alle anagrafiche, con nomi, cognomi, codici fiscali/partite IVA, indirizzi di posta elettronica, numeri di telefono e dati di fatturazione), il Garante ha sottolineato che la non garanzia del protocollo «http» alla riservatezza e all'integrità di tali dati scambiati in rete, oltre che la non possibilità da parte degli utenti di verificare l'autenticità del sito web visualizzato, ha posto in situazione di pericolo il loro trattamento dei loro dati personali.

Dal punto di vista dell'interpretazione della entità sanzione va segnalato che il Garante ha calcolato comunque che l'Azienda non aveva commesso precedenti violazioni analoghe, e ha tenuto un atteggiamento collaborativo nel corso dell'istruttoria.



I.s.e.c. Srl

CHE FARE OPERATIVAMENTE?

Un rapido controllo da farsi riguarda l'indirizzo del vostro sito web, e ove non fosse della forma "**https://www...**" chiedere subito spiegazioni e un intervento alla vostra software house di riferimento perché provveda al più presto al cambio di protocollo. Idem per gli applicativi che consentono ai cittadini di accedere ai vostri servizi on line.

NB. Può essere buona azione inserire tale controllo tra le misure di sicurezza segnalate nel vostro Registro delle Attività di Trattamento.

Siamo a disposizione per ulteriori dettagli, e vi chiediamo di aggiornarci in merito.

Il Data Protection Officer (DPO)