

Comunicazione del DPO/RPD: approfondimento attività condotta dal Garante Protezione Dati Personali - comunicazione n. 12/2022 del 1/04/2022

Con riferimento alle ultime novità inerenti il tema della Protezione dei Personali si segnala come l'Autorità Garante abbia nella settimana che si sta concludendo preso posizione su alcune vicende importanti.

Phishing e cybersicurezza: come ognuno di noi ha potuto osservare, negli scorsi giorni si è verificato un costante incremento ed insidioso incremento delle attività di **phishing**; i messaggi pervenuti consistono in un'imitazione di atti giudiziari ("convocazione giudiziaria", termine privo di giuridica rilevanza) apparentemente provenienti da Enti (Polizia Giudiziaria; Polizia di Stato; Polizia Municipale, ma con domini riconducibili a gmail), mentre in realtà si tratta di una campagna di false email finalizzate a far leva su autorevolezza e paura per sottrarre dati, informazioni o richiedere pagamenti.

Si suggerisce pertanto di non dare seguito a tali messaggi... nemmeno per comunicare il proprio disappunto nel riceverli.

Riservatezza e bilanciamento dei diritti con il diritto di cronaca: il recente caso di cronaca della pubblicazione di contenuti privati intercorsi tra uno Studente di un Liceo e la Dirigente del Liceo stesso offre una necessaria riflessione sul limite tra diritto di cronaca e diritto alla riservatezza; il Garante evidenzia come la protezione di dati personali comporti anche la *necessità di evitare la diffusione di dati ed informazioni ultronei e non necessari*. Il limite dell'essenzialità riguarda quanto collegato ad un interesse pubblico, ma indulgere su circostanze e frasi non aggiunge nulla alla necessità di far chiarezza sui fatti, bensì strizza l'occhio al pruriginoso ed alla (in)giustizia mediatica.

L'intervento del Garante, consistente nel blocco della diffusione, evidenzia come i principi della protezione del dato (ad es. la minimizzazione intesa come stretta necessità) debbano sempre essere osservati da ogni Titolare del trattamento, a prescindere dal contesto in cui si opera.

Possibile Data Breach - Sogei Agenzia Entrate: il problema verificatosi alla Sogei, consistente in un evento accidentale, un mero calo di tensione, ha causato a cascata l'interruzione di numerosi servizi, dalla fatturazione elettronica alla ricette mediche; ad avviso di alcuni importanti studiosi della materia, occorre necessariamente considerare l'evento come una necessaria riflessione sui criteri di sicurezza nella PA.

Sebbene l'evento non sia strettamente un attacco informatico, non di meno ha reso di fatto inservibili numerosi servizi essenziali, ponendo seri dubbi circa la sicurezza del dato, che è comunque stato reso indisponibile in danno dell'Utenza.

Tale situazione, pur non comportando una perdita di riservatezza, è non di meno una perdita di disponibilità, ovvero uno dei tre requisiti fondamentali (riservatezza - disponibilità - integrità) della sicurezza.

L'episodio porta nuovamente a considerare che l'entità di una possibile violazione dei dati personali non si suddivide soltanto in relazione alla volontarietà/non volontarietà dell'evento, ma necessita della valutazione rispetto a tali requisiti (riservatezza; integrità; disponibilità), per poter comprendere in che misura ed in quale grado di gravità la violazione possa avere conseguenze per i diritti degli Interessati.