Cesare Gallotti

****

IT SERVICE MANAGEMENT NEWS – GENNAIO 2018

****

Newsletter mensile con novità in materia di sicurezza delle informazioni, IT Service Management, Qualità.
E' possibile dare il proprio contributo e diffonderla a chiunque.

E' disponibile il blog http://blog.cesaregallotti.it.

La newsletter è inviata via MailUp, offerta da Team Quality S.r.l.

Per iscriversi, cancellarsi e leggere l'informativa privacy:
http://www.cesaregallotti.it/Newsletter.html.

Sulla stessa pagina è possibile consultare l'informativa sul trattamento dei dati personali.

****

Indice

****

01- Nuova privacy per telemarketing

È stata approvata la nuova normativa sulla privcacy in ambito telemarketing. Non ho ancora il numero della norma e pertanto, non avendola ancora letta, evito commenti.

Ivo Trotti di Kantar Italia mi ha segnalato questo articolo da Repubblica:
- http://www.repubblica.it/economia/diritti-e-consumi/diritti-consumatori/2017/12/22/news/telemarketing_e_legge_l_obbligo_di_far_sapere_che_la_telefonata_e_commerciale-184917480/.

Roberto Gallotti (che è anche mio papà) mi ha segnalato questo dal Il Sole 24 Ore:
- http://www.ilsole24ore.com/art/notizie/2018-01-12/privacy-piu-facile-fermare-telefonate-indesiderate-214237.shtml.

****

02- Ritorna la notifica al Garante (nella Legge di Bilancio)

La Legge di Bilancio riporta anche delle indicazioni per la privacy. Faccio riferimento all'articolo 1, commi dal 1020 al 1025 (il comma 1162 fornisce ulteriori fondi al Garante).

La Legge 205 del 2017 si trova su Normattiva:
- www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2017-12-27;205.

Riassumento:
- si ripetono cose già note o comunque prevedibili sul ruolo del Garante (monitoraggio dell'applicazione del GDPR, verifiche, predisposizione di modelli di informativa);
- il Garante dovrà vigilare sulla "presenza di adeguate infrastrutture per l'interoperabilità dei formati con cui i dati sono messi a disposizione dei soggetti interessati, sia ai fini della portabilità dei dati" e quindi spero che capiremo meglio l'estensione del concetto di "portabilità";
- il Garante dovrà "definire linee-guida o buone prassi in materia di trattamento dei dati personali fondato sull'interesse legittimo del titolare"; sicuramente queste saranno utili anche per chi tratta i dati su altri fondamenti legali.

La cosa più inquietante si trova ai commi 2022 e seguenti: "Il titolare, ove effettui un trattamento fondato sull'interesse legittimo che prevede l'uso di nuove tecnologie o di strumenti automatizzati, deve darne tempestiva comunicazione al Garante per la protezione dei dati personali" usando un modello che il Garante metterà a disposizione presumibilmente entro fine febbraio 2018. In caso di silenzio, dopo 15 giorni, il titolare potrà procedere al trattamento, ma il Garante potrà comunque interromperlo (per un massimo di 30 giorni) per chiedere "ulteriori informazioni e integrazioni" o bloccarlo completamente "qualora ritenga che dal trattamento derivi comunque una lesione dei diritti e delle libertà del soggetto interessato"

Perché dico che è inquietante? Perché il GDPR, intenzionalmente, propone l'abrogazione delle "notifiche" al Garante, se non a seguito di PIA (privacy impact assessment) con risultati "negativi". Questo rimette nelle mani del titolare la valutazione della pericolosità dei propri trattamenti, contrariamente a quanto previsto dal Dlgs 196 che richiede, per tutti i trattamenti, la notifica al Garante. Sembrava un passo in avanti, ma il legislatore italiano si è dimostrato ancora una volta troppo paranoico e ha voluto aumentare le normative applicabili e ha voluto reintrodurre un simpatico strumento (la notifica) che speravamo superato.

Da notare un paio di cose:
- la notifica (anche se non si chiama più così) si applica solo ai trattamenti fondati "sull'interesse legittimo", ossia su una delle 6 opzioni su cui fondare un trattamento (legal ground);
- i trattamenti da notificare sono quelli che "prevedono l'uso di nuove tecnologie o di strumenti automatizzati"; ma oggi quasi tutti i trattamenti prevedono l'uso di strumenti automatizzati (notare la "o" disgiuntiva) e quindi la notifica andrà fatta per tutti i trattamenti fondati sull'interesse legittimo del titolare e quindi, per esempio, quelli per protezione aziendale (tutte le attività di videosorveglianza e di log degli strumenti informatici) e per il controllo qualità (quindi tutte le attività di archiviazione pratiche di qualsiasi ufficio, con riportato il nome di chi le ha redatte e approvate).

Sicuramente c'è qualche errore e sarà pubblicata una delle molte "interpretazioni". Però mi pare che l'errore sia grande. A meno che il Garante non voglia crearsi un registro delle imprese italiane.

Grazie a Paolo Calvi e Pietro Calorio degli Idraulici della privacy per la segnalazione.

Paolo Calvi rincara commentando: Così si scardina lo spirito del GDPR, basato sulla responsabilizzazione del titolare, che per trattamenti che rischiano di ledere diritti e libertà

effettua una DPIA, e solo nel caso non riesca a mitigare i rischi si rivolge al Garante con la consultazione prevista dall'art.36. Qui invece sembra si voglia tornare al vecchio meccanismo della notificazione o richiesta di autorizzazione.

****

03- VERA per privacy

Ho pubblicato sul mio sito il VERA per privacy, ossia un foglio di calcolo (Excel) per la valutazione del rischio relativo alla privacy:
- http://www.cesaregallotti.it/Pubblicazioni.html.

Potrebbe essere usata per dimostrare l'adeguatezza delle misure di sicurezza attuate e per realizzare una PIA. Si basa su VERA (Very easy risk assessment), versione 4.4.

Attenzione che questa versione, in italiano, è in versione alfa. Vi prego di inviarmi suggerimenti per il suo miglioramento.

Rispetto al "normale" VERA 4.4:
- aggiornato un poco il foglio di censimento delle informazioni e dei trattamenti;
- aggiunte, nei criteri di valutazione delle informazioni (o dei trattamenti), considerazioni in merito agli impatti sugli interessati (in precedenza si consideravano solo gli impatti sull'organizzazione);
- tolte le minacce senza impatto sulla privacy;
- ridotto il numero di controlli di sicurezza (ossia privacy) a 62 (il VERA 27001 + privacy ne aveva circa 140);
- inserite note (molto sintetiche) per l'interpretazione dei controlli;
- corretto qualche refuso.

Nota: ho apportato qualche piccola correzione ai VERA 4.4 già pubblicati. Essendo pigro, non ho cambiato la versione dei file.

****

04- Nuovo Cad (e conservazione)

A fine 2017 è stata pubblicato un aggiornamento al Codice per l'amministrazione digitale (CAD), che presenta interessanti novità.

Purtroppo non ho ancora disponibile il numero del Decreto (e non capisco neanche se si tratta di un DL o un DLgs) e su Normattiva non vedo il testo consolidato (l'ultima modifica è del novembre 2016).

Per chi vuole portarsi avanti con il lavoro, Franco Ferrari di DNV GL mi ha segnalato due articoli (un terzo lo segnalo qui, ma è citato da uno dei due).

Il primo ha titolo "Conservazione digitale, cosa cambia con il correttivo Cad":
- https://www.agendadigitale.eu/documenti/conservazione-digitale-cosa-cambia-con-il-correttivo-cad/.

Lo trovo molto interessante perché sintetizza efficacemente il processo di accreditamento dei conservatori e i problemi ad esso connessi.

Tra i problemi avrei aggiunto anche considerazioni sulla "perfettibilità" delle liste di riscontro predisposte da AgID e sull'eccessiva onerosità del processo di verifica. Lungi da me volere un processo che permette ai candidati inadeguati di passare la verifica, ma quello attuale è

decisamente eccessivo, dimostrando un eccesso di normazione che diventa, in alcuni casi, inutile.

Gli altri due articoli (titoli "Correttivo CAD, le cinque novità principali" e "Il CAD numero 6 è in Gazzetta Ufficiale, che succede ora") contengono informazioni utili:
- https://www.agendadigitale.eu/cultura-digitale/correttivo-cad-le-cinque-novita-principali/;
- https://www.agendadigitale.eu/cittadinanza-digitale/il-cad-numero-6-e-in-gazzetta-ufficiale-che-succede-ora/.

****

05- Tutelato il dipendente che segnala illeciti

Segnalo questa novità dal sito di Altalex: "Whistleblowing, in vigore le nuove norme: tutelato il dipendente che segnala illeciti":
- http://www.altalex.com/documents/leggi/2017/11/16/whistleblowing.

Copio e incollo: "il dipendente che segnala al responsabile della prevenzione della corruzione dell'ente o all'Autorità nazionale anticorruzione o ancora all'autorità giudiziaria ordinaria o contabile le condotte illecite o di abuso di cui sia venuto a conoscenza in ragione del suo rapporto di lavoro, non può essere - per motivi collegati alla segnalazione - soggetto a sanzioni, demansionato, licenziato, trasferito o sottoposto a altre misure organizzative che abbiano un effetto negativo sulle condizioni di lavoro".

Inoltre: "Le nuove disposizioni valgono anche per chi lavora in imprese che forniscono beni e servizi alla Pa".

****

06- Pubblicata la nuova versione della SP 800-160 (Systems Security Engineering)

Il NIST ha pubblicato la nuova versione della SP 800-160 dal titolo "Systems Security Engineering":
- https://csrc.nist.gov/publications/detail/sp/800-160/final.

Confesso di non averla letta (è un malloppo di 160 pagine), ma ne avevo letto le versioni precedenti e non riesco a individuare i cambiamenti in questa (tranne gli errata, riportati in tabella). Sicuramente è un documento importante per chiunque si occupa di sicurezza.

****

07- La vulnerabilità di inizio 2018 in realtà è doppia e si chiama Spectre e Meltdown.

Per ora il migliore articolo tecnico l'ho trovato sul National Cyber Security Centre (del GCHQ):
- https://www.ncsc.gov.uk/guidance/meltdown-and-spectre-guidance.

Trovo utile ricordare che:
- sono vulnerabili tutti i dispositivi e quindi è necessario aggiornare quelli personali (pc e smartphone), i server, gli apparati di rete (router, firewall, eccetera);
- i server includono gli hypervisor e le guest machine; in altre parole, chi ha i servizi "in IaaS sul cloud" non può ignorare il problema (questo conferma ancora una volta che chi usa servizi cloud deve comunque mantenere forti competenze al proprio interno);
- anche i compilatori vanno aggiornati e, dopo, tutto quanto compilato va ricompilato (questa verifica di sicurezza è fatta raramente, credo, anche perché oggi sono pochi i software compilati; ciò non ostante questo punto andrebbe meglio valutato in futuro).

La questione è esplosa su tutti i media. Passa un po' inosservato il fatto che "non risultano siano stati condotti con successo attacchi che sfruttano queste vulnerabilità". Quindi alcuni suggeriscono di affrontare queste vulnerabilità, ma senza entrare in "panic mode".

****