Cesare Gallotti

****
IT SERVICE MANAGEMENT NEWS – FEBBRAIO 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- GDPR: ENISA Handbook

ENISA ha pubblicato a gennaio 2018 un "Handbook on Security of Personal Data Processing":
- https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing/.

In esso trovo cose interessanti:
- la valutazione del rischio per i processi (con i parametri di valutazione degli impatti e della verosimiglianza delle minacce);
- un elenco di misure di sicurezza da considerare per i diversi livelli di rischio.

Mi pare un documento molto interessante perché molto pratico (a differenza di altre pubblicazioni troppo "teoriche").

Alla luce di questo documento dovrò aggiornare il mio VERA per privacy (ahimè).

Meno interessante è la pubblicazione "Privacy and data protection in mobile applications", perché troppo analitica e con poche indicazioni per la sicurezza delle applicazioni per dispositivi mobili:
- https://www.enisa.europa.eu/publications/privacy-and-data-protection-in-mobile-applications/.

Da osservare comunque che la pubblicazione è piena di link ad altri documenti. Andrebbe quindi esaminata con attenzione.

****
02- GDPR: Un riassunto (e il quaderno ANCI)

In tanti (tra cui Franco Ferrari di DNV GL, Pierfrancesco Maistrello e Daniela degli Idraulici della privacy) hanno segnalato questo quaderno dell'ANCI dal titolo "L'attuazione negli Enti Locali del nuovo Regolamento UE n. 679/2016 sulla protezione dei dati personali: Istruzioni tecniche, linee guida, note e modulistica":
- http://www.anci.lombardia.it/documenti/7355-regolamento%20ue%20privacy%20ok_def.pdf.

Può essere utile criticarlo, in modo da fare un ripasso di alcuni punti salienti del GDPR. Così potrò essere criticato anche io per quello che scrivo.

Innanzi tutto prima dice che "è definita la nuova categoria di dati personali", che sono i cosiddetti "dati sensibili di cui al precedente Codice Privacy". Poi tutto il quaderno fa riferimento ai "dati sensibili". Il GDPR usa l'espressione "categorie particolari di dati personali ai sensi dell'articolo 9". Anche io uso l'espressione "dati sensibili" perché più pratica, avendo cura, a inizio di documento, di specificare cosa sono e come li designa il GDPR.

I Titolari e i Responsabili dei trattamenti sono visti come persone fisiche (dice che il titolare è il "Sindaco o suo delegato" e i responsabili sono "Dirigenti/Quadri/Responsabili di U.O."), mentre il GDPR lascia intendere che si tratta di strutture organizzative (le "aziende"), mentre le responsabilità personali, tranne il caso di singoli professionisti, sono da gestire con le normali deleghe interne di ciascuna organizzazione e non sono regolamentate dal GDPR. Per la verità non avrebbero dovuto essere regolate neanche dal Codice privacy e questo sarebbe stato più chiaro se non si fosse tradotto "processor" (che anche in altri contesti è sempre visto come organizzazione non singola persona) con "responsabile" e se poi non avessimo insistito per lasciare in vita la traduzione inesatta. Questa interpretazione è stata data anche da dirigenti e funzionari del GDP in diversi incontri pubblici, dicendo che negli anni hanno sempre visto il "responsabile interno" come figura non prevista dal Codice e il "responsabile esterno" come "responsabile e basta" (potevano scriverlo da qualche parte, visto che scrivono già tanto, così avremmo fatto meglio e io non avrei scritto alcune sciocchezze in passato; purtroppo non mi sembrano abbiano intenzione di scriverlo neanche in futuro).

Non sono competente di regolamenti comunali. Quello proposto, a mio parere, manca completamente di regole in merito alle misure di sicurezza da adottare (si limita a parlare di sistema di autorizzazione e di sistema antincendio).

Troppa enfasi è ancora data al consenso come base legale per il trattamento. Oggi sappiamo che le basi legali sono di 6 tipi.

Si sono dimenticati i trattamenti relativi al personale del Comune. Certamente i dati dei cittadini sono importantissimi e devono costituire il punto di maggiore attenzione per i Comuni quando si parla di protezione dei dati personali, però non trovo corretto dimenticarsi completamente dei dati del personale.

Interpreta in modo bizzarro il ruolo degli "incaricati" secondo il Codice privacy, dicendo che sono "sub-responsabili del trattamento". Non posso condividere questa lettura. Mi pare, anzi, che non venga colta la possibilità di designare gli incaricati (ossia autorizzare le persone a trattare i dati personali) in modo adeguato alle esigenze di controllo (reale) e efficienza ma, anzi, promuova il "vecchio" metodo basato su lettera formale firmate e controfirmata.

Ancora più bizzarramente prevede che il Titolare possa delegare un responsabile a nominare il DPO ("alla designazione del Responsabile per la Protezione dei Dati (RPD), se a ciò demandato dal Titolare"). Altra lettura che non posso condividere.

Mi ha fatto notare Pierfrancesco Maistrello che viene suggerita la tenuta di più registri dei trattamenti. Ancora una volta non posso condividere questo approccio.

L'ultima parte del documento (da pagina 43 a pagina 78) è costituita dalla "Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali" del Garante privacy. Lettura sempre utile.

PS: Francesco Pizzetti e Luca Leone, su LinkedIn hanno commentato dicendo che non bisognerebbe mai usare l'espressione "dati sensibili". Personalmente non vedo ragione oltre la purezza formale. Ho chiesto. Se avrò risposta, la diffonderò.

****

03- GDPR: una sfida per le Autorità di controllo

Segnalo questo articolo (22 pagine) di Francesco Pizzetti dal titolo "La protezione dei dati personali dalla direttiva al nuovo regolamento: una sfida per le Autorità di controllo e una difesa per la libertà dei moderni":
- http://www.medialaws.eu/rivista/la-protezione-dei-dati-personali-dalla-direttiva-al-nuovo-regolamento-una-sfida-per-le-autorita-di-controllo-e-una-difesa-per-la-liberta-dei-moderni/.

Non è un articolo "pratico", a differenza di qualche intervento di Pizzetti a dei convegni e che avrei voluto vedere per iscritto. È una riflessione, come dice il titolo, sul ruolo del Garante.

****

04- Privacy: Nuova privacy per telemarketing (precisazione)

A gennaio avevo dato la notizia di un nuovo provvedimento normativo su privacy e telemarketing:
- http://blog.cesaregallotti.it/2018/01/nuova-privacy-per-telemarketing.html.

Mancava il numero della Legge. Grazie ad Altalex ora posso dire che si tratta della Legge 5 del 2018:
- http://www.altalex.com/documents/leggi/2018/02/05/call-center-prefissi-registro-opposizioni.

Come al solito, si trova su Normattiva:
- www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2018-01-11;5!vig=.

****

05- Privacy: Due sentenze sul controllo dei lavoratori (uso cellulari e videoriprese per furti)

Due sentenze che sembrano interessanti, ambedue su Filodiritto.

La prima è una "verifica preliminare" del Garante e relativa al controllo dei consumi del cellulari aziendali. La società (Johnson&Johnson Medical S.p.A.) assicura che i dati saranno usati solo per il controllo dei consumi e non per comminare sanzioni disciplinari. Il Garante ha dato l'approvazione:
- http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7554790.

L'articolo su Filodiritto:
- https://www.filodiritto.com/news/2018/privacy-garante-privacy-il-garante-si-pronuncia-sulla-legittimit-del-controllo-sui-telefoni-aziendali-da-parte-del.html.

La seconda è della Cassazione, che ha ritenuto lecito l'uso di videoregistrazioni "per provare le condotte criminose poste in essere dai lavoratori". Da notare che si sta parlando di procedura penale. L'articolo di Filodiritto:
- https://www.filodiritto.com/news/2018/videosorveglianza-cassazione-penale-utilizzabili-le-videoriprese-per-provare-le-condotte-criminose-poste-in-essere-dai.html.

****
06- Privacy: Sentenza su dati sensibili e cifratura

La notizia me l'ha data per primo Luca De Grazia, ma confesso che non ci avevo capito molto.

L'ho ritrovata su Altalex e quindi ho cercato di capirla meglio:
- http://www.altalex.com/documents/news/2018/01/09/privacy-banca-dati-sensibili.

Una persona si lamenta perché l'accredito sul suo estratto di conto corrente riporta nella causale la motivazione (il numero di Legge, che però riguarda due specifici casi sanitari). A fronte di questo, la Cassazione ha deciso che:
a) la Regione Campania (che ha fatto l'accredito) deve cifrare i dati, in quanto è previsto che i soggetti pubblici debbano cifrare i dati pesonali sanitari dal D. Lgs. 196 del 2003;
b) in forza di questo, anche la banca deve cifrare i dati personali sanitari.

A mio parere era già inappropriato chiedere agli enti pubblici di cifrare i dati personali sanitari, senza rendersi conto degli impatti di tale misura, la sua sostanziale inutilità e prevedendo differenza tra il pubblico e il privato.

Però qui i giudici si sono ritrovati davanti ad un problema, visto che un'altra normativa (un Regio Decreto del 1924!) impone di specificare nei mandati di pagamento la precisa indicazione dell'oggetto di spesa. Ma allora, se è richiesto di cifrarla, come sarebbe riportata nell'estratto conto del destinatario?

Mi rifiuto di studiare l' art. 409 del R.D. n. 827 del 1924, ma credo proprio che un'altra soluzione si renderà necessaria. O forse no?

****

07- Standard: ISO/IEC 27000:2018

E' stata pubblicata la nuova versione del 2018 della ISO/IEC 27000, con i termini e definizioni della sicurezza delle informazioni:
- https://www.iso.org/standard/73906.html.

La norma è gratuita, quindi dalla pagina dell'ISO non bisogna "comprare", ma seguire il link di "download". Il download si può anche fare direttamente da questa pagina:
- http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html.

****
08- Standard: Circolare Accredia per le certificazioni ISO/IEC 270XX

Come già detto più volte in questa sede, la ISO/IEC 27001 può essere "estesa" ad altre norme cosiddette sector-specific. Tra queste, le più note sono oggi la ISO/IEC 27108:2014 sulla privacy dei servizi cloud e la ISO/IEC 27017 sui servizi cloud in generale. Altre sono disponibili e altre lo saranno (inclusa la ISO/IEC 27552 sulla privacy in generale).

In poche parole: non è possibile certificarsi direttamente su queste norme sector-specific, ma è possibile farle figurare in un certificato ISO/IEC 27001, come sua estensione.

Accredia, l'ente di accreditamento italiano, aveva regolato qualche mese fa le certificazioni ISO/IEC 27018. Io mi ero lamentato perché era assurda questa limitazione ad una sola delle norme sector-specific:
- http://blog.cesaregallotti.it/2017/07/certificazioni-isoiec-27018.html.

Accredia ha quindi rimediato (probabilmente non a causa mia) con la Circolare Tecnica N° 02/2018:
- https://www.accredia.it/documento/circolare-tecnica-dc-n-02-2018-accreditamento-per-lo-schema-di-certificazione-iso-iec-270012013-con-integrazione-delle-linee-guida-iso-iec-270xx20yy/.

Rimangono alcune bizzarrie, come richiedere auditor competenti anche sulla ISO/IEC 20000 (chissà perché questa e non per esempio la ISO 22301 o altre) e di verificare fisicamente tutti i data centre utilizzati (senza alcuna deroga nel caso in cui questi siano già certificati). Speriamo che in una prossima versione della Circolare tecnica non ci siano queste bizzarie.

****
09- Standard: ISO 45001 sulla sicurezza dei lavoratori

Segnalo che è stata approvata e sarà tra poco disponibile la ISO 45001 dal titolo "Occupational health and safety management systems -- Requirements with guidance for use":
- https://www.iso.org/standard/63787.html.

Io non mi occupo di questa materia, ma credo sia importante sapere dell'esistenza di questo standard, visto che questa materia si interseca con la sicurezza delle informazioni.

****

10- Servizi eIDAS: Nuovo Cad (e conservazione) - Riferimenti corretti

In un precedente post avevo segnalato gli aggiornamenti al CAD, senza però fornire i riferimenti normativi esatti:
- http://blog.cesaregallotti.it/2018/01/nuovo-cad-e-conservazione.html.

I riferimenti normativi mi sono stati forniti da Luca De Grazie e Franco Ruggieri, che ringrazio. Il CAD (D.Lgs. 82 del 2005) è stato modificato, con decorrenza 18 gennaio 2018, dal D. Lgs. 217 del 2017.

Il nuovo CAD è disponibile su Normattiva:
- www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2005-03-07;82!vig=

NB: il link diretto non sembra funzionare; è necessario copiarlo e incollarlo.

****
11- Servizi eIDAS: Servizio Serc, la forse futura PEC

Franco Ferrari del DNV GL mi ha segnalato questo articolo che presenta il SERC (Servizio elettronico di recapito certificato):
- https://www.agendadigitale.eu/cittadinanza-digitale/servizio-elettronico-recapito-certificato-cose-perche-pensionare-la-pec/.

Forse un giorno questo servizio, previsto dal Regolamento eIDAS, sostituirà la PEC. Per intanto: gli standard tecnici saranno pronti (forse) per febbraio 2019. Ma credo sia giusto informarsi, almeno un po', di cosa si tratta.

****
12- Le basi della digital forensics (per la GdF ma non solo)

Segnalo questo articolo di Paolo Dal Checco dal titolo "Le basi della digital forensics nella circolare 1/2018 della Guardia di Finanza":
- https://www.ictsecuritymagazine.com/articoli/le-basi-della-digital-forensics-nella-circolare-12018-della-guardia-finanza/.

Penso sia un ottimo articolo di introduzione (e anche di approfondimento) sulla digital forensics, che prende spunto da una circolare della GdF.

****
13- Sviluppo sicuro delle applicazioni: due miei articoli (il processo e i test di sicurezza)

Segnalo il mio ultimo articolo su ICT Security dal titolo "Sviluppo sicuro delle applicazioni: il processo":
- https://www.ictsecuritymagazine.com/articoli/sviluppo-sicuro-delle-applicazioni-processo/.

Un altro articolo ha titolo "Sviluppo sicuro delle applicazioni: i test di sicurezza":
- https://www.ictsecuritymagazine.com/articoli/sviluppo-sicuro-delle-applicazioni-test-sicurezza/

Ne approfitto per segnalare che sono a corto di idee. Se qualcuno ha degli argomenti da suggerirmi, lo invito a farlo.

****

14- Linee guida AgID sullo sviluppo sicuro

Franco Ferrari di DNV GL mi ha segnalato la pubblicazione, da parte di AgID, delle "Linee guida per lo sviluppo del software sicuro":
- http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/cert-pa/linee-guida-sviluppo-sicuro.

Le ho sfogliate rapidamente e mi sembrano un lavoro di "compilazione", ossia di raccolta di varie metodologie, pratiche e linee guida. Si rimane un po' storditi dalla mole di materiale.

A questo si aggiunga che molte indicazioni, sopratuttto quelle di processo, sono quelle classiche da teorici: belle, rigorose e... estremamente onerose.

Se però si ha la pazienza di scorrerle, si trovano molte cose interessanti (a me hanno colpito soprattutto i paragrafi con le tecniche di codifica per i singoli linguaggi). Si aggiunga che non mi pare siano disponibili lavori simili e quindi questo è utilissimo per quanto vogliono studiare lo sviluppo sicuro oltre le Top 10 di OWASP.

****

15- Perfect SAP Penetration testing

Recentemente ho chiuso un progetto ISO/IEC 27001 in un'azienda molto "sappizzata". Questa serie di articoli, dal titolo "Perfect SAP Penetration testing" mi sarebbe tornata decisamente utile:
- https://erpscan.com/tag/sap-penetration-testing/.

****

16- Articolo su DR per piccole e medie imprese

Tom Keller, autore di questo articolo dal titolo "How to Disaster-Proof Your Business IT", mi ha contattato per presentarmelo:
- https://digital.com/blog/disaster-proof/.

Nulla di eccezionale, ma tutto corretto e, soprattutto, con il tono giusto: tecnico senza tragedie o esaltazioni.

Alla fine dell'articolo ci sono dei link. Quello più interessante è quello verso www.smallbusinesscomputing.com, che a sua volta presenta dei link a soluzioni di mercato.

Attenzione però ad una cosa: noi europei dobbiamo, preferibilmente e per evitare le complicazioni del GDPR, usare server in EU e non tutte le soluzioni proposte garantiscono questo aspetto.

****

17- Libro bianco della cyber security in Italia

Franco Ferrari di DNV GL mi ha segnalato questo articolo dal titolo "Cybersecurity, ecco il Libro bianco (ma anche il Libro verde) sulla strategia italiana":
- https://www.corrierecomunicazioni.it/cyber-security/cybersecurity-libro-bianco-anche-libro-verde-sulla-strategia-italiana/.

Certo... l'autore sembra decisamente troppo entusiasta (sembra quasi abbia un debito di riconoscenza con qualcuno degli autori). E si dimentica di dare un link dove reperirlo. Eccolo qui:
- https://www.consorzio-cini.it/index.php/it/labcs-home/libro-bianco.

A me il link non funziona. Quindi l'ho trovato sul sito del Sole 24 Ore: http://www.ilsole24ore.com/pdf2010/Editrice/ILSOLE24ORE/ILSOLE24ORE/Online/_Oggetti_Correlati/Documenti/Notizie/2015/11/CyberSecurity-Report.pdf.

L'ho letto rapidamente. Sembra ci siano dentro le "solite" (ma non per questo sbagliate o inattuali) idee e più un tono giornalistico che scientifico. Forse chi è più paziente di me se lo leggerà con attenzione e potrà segnalarci i punti più rilevanti (se già non evidenziati dall'articolo segnalato).