Cesare Gallotti

****
IT SERVICE MANAGEMENT NEWS – SETTEMBRE 2020
****

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 si trova l'informativa sul trattamento dei dati personali.

****
Indice

****
01- Pubblicato "Un piccolo libro sulla privacy, il GDPR e come attuarlo"

Lo trovate in formato digitale (consiglio il sito della piattaforma di auto-pubblicazione che abbiamo usato):
- https://store.streetlib.com/it/idraulici-della-privacy/un-piccolo-libro-sulla-privacy-il-gdpr-e-come-attuarlo.

In formato cartaceo (su un'altra piattaforma di auto-pubblicazione che abbiamo usato):
- https://www.lulu.com/it/shop/idraulici-della-privacy-/un-piccolo-libro-sulla-privacy-il-gdpr-e-come-attuarlo/paperback/product-m5gq84.html.

Qualcuno vuole leggere la quarta di copertina? Eccola: "Un libro breve e di taglio pratico (poca teoria, molti esempi) su come applicare il GDPR.

Gli Idraulici della privacy sono un gruppo selezionato di consulenti e manager in ambito della protezione dei dati personali che quotidianamente si sporcano le mani per affrontare, se serve anche con spirito da artigiani, le necessità dei propri clienti o colleghi. I membri del gruppo condividono le criticità che incontrano, propongono interpretazioni normative, si scambiano e raccontano esperienze ed elaborano chiavi di lettura sulle più varie e diverse tematiche privacy. Questo confronto costante permette al singolo professionista di arricchire le proprie conoscenze, gli strumenti e le soluzioni a sua disposizione per risolvere anche le situazioni più spinose.

Il ricavato di questo libro, completato nella prima metà del 2020 durante l'emergenza COVID-19, sarà devoluto in beneficenza".

I membri del gruppo (potete poi chiamarci per nome, come per i Beatles): Cesare Gallotti (curatore), Glauco Rampogna (revisore e curatore dell'epub), Stefania Algerio, Elia Barbujani, Fulvia Emegian, Pierfrancesco Maistrello, Ferruccio Militello, Nicola Nuti, Monica Perego, Manuel A. Salvi.

****

02- Stato delle norme ISO/IEC 270xx - Settembre 2020

Si è appena concluso il 63mo meeting dell'ISO/IEC JTC 1 SC 27. Doveva essere a Varsavia, ma si è invece tenuto tutto in ambiente virtuale.

La delegazione italiana era composta da 7 persone, tra cui: Fabio Guasconi (Presidente, che ringrazio per avermi segnalato qualche errore in questo mio commento), Alessandro Cosenza e me stesso.

Ricordo che gli stati delle norme sono: WD - CD - DIS - FDIS - IS (pubblicazione).

Per quanto riguarda le norme del WG 1, non ci sono grosse novità. Mi limito, come al solito, ad indicare lo stato di avanzamento di alcune norme
- ISO/IEC 27002 (controlli di sicurezza): sono proseguiti i lavori e la norma è rimasta in stato CD e si spera di pubblicarla a ottobre 2021;
- ISO/IEC 27005 (sul risk management): sono proseguiti i lavori e la norma è rimasta in stato di CD; ancora una volta è oggetto di molte discussioni, e si spera di pubblicarla entro dicembre 2022 (due finale!);
- ISO/IEC 27013 (relazioni tra ISO/IEC 20000-1 e ISO/IEC 27001): sono proseguiti i lavori, passa in stato DIS e si spera di pubblicare entro dicembre 2021.

A breve verranno pubblicate le norme ISO/IC 27101 (sullo sviluppo di framework di cybersecurity) e 27022 (sui processi di sicurezza delle informazioni), ma non ne ho seguito i lavori.

La norma con i requisiti di accreditamento degli organismi di certificazione per svolgere gli audit ISO/IEC 27701 era denominata ISO/IEC 27558 e sarà sicuramente rinominata

ISO/IEC 27006-2. Sarà pubblicata entro fine anno.

La ISO/IEC 27006-2 sarà una Technical specification. I lavori sono stati fatti molto in fretta al fine di regolamentare quanto prima un mercato potenzialmente molto vasto. Ci sono alcune cose che ho apprezzato, altre meno e altre ancora che saranno migliorate nelle future edizioni, ma per intanto abbiamo una buona norma per avviare le certificazioni ISO/IEC 27701 accreditate.

La ISO/IEC 27006 sarà numerata ISO/IEC 27006-1 e partiranno i lavori di revisione.

Per quanto riguarda le norme del WG 5 (privacy), segnalo:
- per la ISO/IEC 29134 (sulla PIA) è stato proposto un amendement, ma solo per questioni puramente formali (a mio parere scorrettamente, in quanto non è possibile fare più di 2 Amendement e già altre volte sono stati riscontrati errori sostanziali per cui non era più possibile produrre correzioni);
- ho partecipato, anche se troppo poco, alle interessantissime discussioni sulla norma ISO/IEC 27557 (che uscirà non prima di fine 2022) incentrata sul "rischio privacy organizzativo", distinguendo così tra valutazioni del rischio privacy per l'organizzazione e per gli interessati.

Per il WG 4, che si occupa di norme più tecniche, ho smesso di interessarmi a quelle sull'IoT perché non c'è un vero senso di direzione e i documenti finora prodotti sono troppo teorici. Da questo punto di vista, preferisco seguire i lavori di ENISA.

Il prossimo meeting sarà ad aprile a Sanpietroburgo o nel cyberspazio, a seconda di come andrà l'emergenza COVID.

****

03- Pubblicata la IEC 62443-3-2 per la valutazione del rischio per i sistemi IACS (OT)

E' stata pubblicata a giugno 2020 la norma "Security for industrial automation and control systems - Part 3-2: Security risk assessment for system design":
- https://webstore.iec.ch/publication/30727.

Essa presenta I requisiti per una valutazione del rischio tecnica dei sistemi informatici industriali (normalmente indicati come OT, ma indicati dalla norma IACS).

Ricordo che la 62443 è divisa in più parti: la prima per i concetti generali, la seconda per i sistemi di gestione, la terza per i sistemi OT e la quarta per le singole componenti.

Trovo interessante l'approccio di questa 62443-3-2 perché richiede di suddividere opportunamente il sistema in sottosistemi, in modo da assicurarne coerenza.

Alcune zone da tenere separate sono: sistemi di business, IACS, sistemi di sicurezza fisica delle persone (safety), dispositivi connessi temporaneamente, i dispositivi wireless, i dispositivi connessi da reti esterne.

****

04- Nuove linee guida AgID sulla gestione dei documenti informatici

A inizio settembre AgID ha pubblicato una nuova edizione delle "Linee Guida sulla formazione, gestione e conservazione dei documenti informatici":
- https://trasparenza.agid.gov.it/archivio19_regolamenti_0_5385.html.

Ho cercato di capire la questione con Franco Vincenzo Ferrari di DNV GL. Grazie a lui, vi segnalo questo articolo che secondo me è il più chiaro e completo in merito ai cambiamenti intervenuti sulla materia, di interesse per il pubblico e per il privato: https://www.agendadigitale.eu/documenti/conservazione-dei-documenti-ecco-tutte-le-regole-nelle-linee-guida-agid/.

****

05- Decreto semplificazioni

Il 17 luglio è entrato in vigore il DL 76/2020, detto "DL Semplificazione". Ci sono molte novità in materia di informatica e per queste segnalo l'articolo dal titolo " DL semplificazione 2020 cambia la PA digitale: ecco come":
- https://www.agendadigitale.eu/cittadinanza-digitale/dl-semplificazione-2020-come-cambia-la-pa-digitale/.

Sempre su Agenda Digitale ci sono altri articoli di Manca su questa materia e ne raccomando la lettura a chi ne è interessato.

Franco Vincenzo Ferrari di DNV GL mi ha raccomandato questo articolo dal titolo "DL Semplificazioni e conservazione dei documenti informatici delle PA: cosa cambia":
- https://www.agendadigitale.eu/cittadinanza-digitale/dl-semplificazione-2020-come-cambia-la-pa-digitale/.

In materia di conservazione, mi pare che si possa riassumere la situazione attuale con questo capoverso: "La sostanza delle modifiche necessarie si avrà solo dopo due provvedimenti attuativi in capo ad AgID", uno dei quali è proprio quello indicato nell'articolo precedente questo.

Il 10 settembre è stata approvata la conversione in Legge. Ulteriori riflessioni potranno quindi essere fatte quando sarà disponibile su Normattiva (www.normattiva.it) il testo definitivo o quando ci saranno articoli interessanti.

****

06- US Clean network program

Sandro Sanna mi ha segnalto alcuni articoli in merito all'US Clean network program.

Il primo è in Italiano e ha titolo "Trump firma il decreto che vieta TikTok e WeChat negli Stati Uniti":
- http://amp.ilsole24ore.com/pagina/ADR3pLi.

Il secondo è la pagina sull'iniziativa The Clean Network dell'US Department of State, ovviamente favorevole all'iniziativa:
- https://www.state.gov/the-clean-network/.

Il terzo è molto critico sull'iniziativa e ha titolo "The Hidden, Dirty Secrets Behind the US Clean Network Program" (e mi si scusi, ma mi lascia stranito il fatto che l'autore abbia un nome che suona cinese; non metto in dubbio le sue competenze e la sua integrità, ma tutto suona assurdo):
- https://www.globaltimes.cn/content/1197211.shtml.

Pensavo di non aver nulla da dire in merito, anche perché non so nulla in merito. So solo che la guerra sul 5G non è tanto sulla sicurezza, ma economica (visto che ovviamente l'acquisto di apparati 5G fatti negli USA favorirebbe l'industria statunitense!) e che puntare il dito sui social e sugli IM cinesi non toglie i dubbi sui social e sugli IM statunitensi.

Ed è proprio su queste cose che ho un'idea strana nella testa: perché ci facciamo tante paranoie sulla sicurezza dei servizi cinesi (e anche a quelli italiani) e invece diamo tutti i nostri dati agli statuntensi? Le aziende usano sempre più i servizi pubblici e gratuiti, anche per scambiarsi dati molto critici, senza pensare a quanto questi siano oggetto di analisi da parte di soggetti non identificati. Ecco quindi che penso che dovremmo farci un "programma di pulizia informatica" anche in casa e in azienda. Ma non è per niente facile e forse, oggi, impossibile.

****

07- Valutazione del rischio dei fornitori: strumento del NIST

Il NIST ha recentemente pubblicato il documento NISTIR 8272 "Impact Analysis Tool for Interdependent Cyber Supply Chain Risks":
- https://csrc.nist.gov/publications/detail/nistir/8272/final.

Il documento è accompagnato da un applicativo per Windows, Mac OS e Linux.

Non sono riuscito ad approfondire molto l'approccio perché dovrei soprattutto avere modo di usare lo strumento. Ad una prima lettura mi sembra valido, anche se ho sempre molte riserve quando si tratta di "tool per la valutazione del rischio".

Penso però che possa essere significativo per realtà di grandi dimensioni, coinvolte in numerosi progetti IT o con molti prodotti IT da acquistare e dove l'investimento nell'analisi permette di allocare correttamente le risorse per controllare il rischio; per realtà di piccole o medie dimensioni, dove analisi complesse non forniscono informazioni significative, è sicuramente consigliabile un approccio molto più snello, visto che è più semplice vedere dove il rischio è più elevato e quindi dove investire più risorse per controllarlo.

****

08- Analisi Microsoft sul lavoro da remoto

Segnalo questo interessante post di Nicola Vanin su LinkedIn, dove riassume i risultati di un'analisi interna di Microsoft presso il proprio personale in merito al lavoro da remoto (il cosiddetto "smart working"):
- https://www.linkedin.com/posts/nicola-vanin-b03a5451_microsoft-brutale-infinita-activity-6693148405046280192-BNPx.

Aggiungo solo che la ricerca completa di Microsoft si trova qui:
- https://insights.office.com/workplace-analytics/microsoft-analyzed-data-on-its-newly-remote-workforce/.

****

09- Linee guida EDPB su titolare e responsabile

L'EDPB ha adottato il 2 settembre le "Guidelines 07/2020 on the concepts of controller and processor in the GDPR":
- https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en.

Sono decisamente importanti e dovrebbero essere sotto mano ogni volta.

Ancora oggi trovo organizzazioni per cui i responsabili sono quelli interni, mentre queste linee guida, per esempio, dicono che il responsabile è un'entità distinta rispetto al titolare.

Al momento in cui scrivo non mi risulta che sia stata ancora preparata una traduzione in italiano.

Il 18 luglio avevo segnalato le linee guida del novembre 2019 sul medesimo argomento dell'EDPS, ma ritengo che queste siano più significative, almeno perché successive.

****

10- Requisiti per l'accreditamento degli OdC per le certificazioni GDPR

Il 29 luglio 2020, il Garante per la privacy ha approvato la delibera con titolo "Requisiti aggiuntivi di accreditamento degli organismi di certificazione":
- https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9445086.

Li ho letti molto superficialmente perché si tratta dei requisiti per gli organismi di certificazione e non per organizzazioni che intendono ottenere un "bollino GDPR". Certamente è utile e interessante sapere che si stanno facendo passi avanti verso l'attivazione di un meccanismo di certificazione, ma questa deve ancora avvenire.

Infatti mancano i "criteri approvati dal Garante o dal Comitato europeo per la protezione dei dati (di seguito "Comitato") in conformità dell'articolo 43, paragrafo 2, lettera b) e dell'articolo 42, paragrafo 5 del Regolamento", ossia i requisiti che devono rispettare i servizi (o i processi o i prodotti) da certificare.

Sottolineo che, con il testo sopra riportato, la Delibera ribadisce il fatto che i criteri devono essere approvati dal Garante o dall'EDPB, non da altre entità (p.e. Accredia, che su questo argomento ha già fatto un passo falso qualche tempo fa).

Quindi: a meno che non lavoriate per un organismo di certificazione, è inutile che vi agitiate. Ovviamente è utile tenere monitorata la situazione.

Ringrazio Monica Perego che, incurante della prossimità a Ferragosto, ha dato la notizia agli Idraulici della privacy il 13 agosto e a Franco Ferrari di DNV GL che invece me l'ha comunicata il 4 settembre.

****

11- Invalidato il Privacy Shield - Le FAQ dell'EDPB

L'EDPB (ossia l'organismo di cooperazione dei garanti privacy europei) ha pubblicato le FAQ sulla sentenza Schrems II, che pone molti limiti sui trasferimenti di dati personali negli USA:
- https://edpb.europa.eu/our-work-tools/our-documents/other/frequently-asked-questions-judgment-court-justice-european-union_en.

Grazie a Chiara Ponti degli Idraulici della privacy per aver condiviso il link.

Sicuramente i trasferimenti sotto Privacy shield non sono più validi. Anzi, sono illegali sin dal 16 luglio 2020.

Come ho già scritto, potrebbero essere usate le SCC (Standard contractual clauses o, in italiano, Clausole contrattuali tipo), ma anche quelle hanno dei problemi perché se la legislazione del Paese importatore non offre le garanzie legali presenti in Europa, un contratto tra privati non può migliorare la situazione. Stessa questione per le BCR (Binding corporate rules o, in italiano, norme vincolanti d'impresa).

Mi sembra che i capoversi fondamentali del documento dell'EDPB siano: "The EDPB is currently analysing the Court's judgment to determine the kind of supplementary measures that could be provided in addition to SCCs or BCRs, whether legal, technical or organisational measures, to transfer data to third countries where SCCs or BCRs will not provide the sufficient level of guarantees on their own. The EDPB is looking further into what these supplementary measures could consist of and will provide more guidance".

Traduco: se non sanno loro cosa fare per assicurare la validità delle SCC e BCR anche in Paesi con legislazione che non assicura un adeguato livello di protezione ai dati personali, io aspetto che lo sappiano e ce lo dicano.

Infine non mi pare dica niente sulle società di servizi informatici statunitensi che però assicurano l'uso di data center in Europa. E' sufficiente questa garanzia sull'uso di data center in Europa o no? Bisogna infatti dire che molti contratti con questi grandi fornitori di servizi IT non assicurano il completo rispetto della locazione geografica, come indicato dall'analisi di EDPS sui servizi Microsoft (che avevo già segnalato a suo

tempo):
- https://edps.europa.eu/sites/edp/files/publication/20-07-02_edps_euis_microsoft_contract_investigation_en.html.

Segnalo un interessantissimo post di Nicola Vanin su LinkedIn dal titolo "Chi sta trasmettendo ancora dati personali negli USA?":
- https://www.linkedin.com/posts/nicola-vanin-b03a5451_trasmettendo-personali-usa-activity-6701723919822462976-FCHA.

****

12- Foto del registro accessi (violazioni)

Mi dicono che un'associazione ha denunciato una violazione di dati personali (data breach) al Garante perché un socio ha fotografato il registro degli accessi.

Mi sembra che la decisione di inoltrare la notifica al Garante sia un po' eccessiva, ma sappiamo bene che la paura (ingiustificata, a mio parere, in questo caso) di sanzioni porta a questo e altro.

Però... io in questo vedo alcune piccole lezioni di sicurezza delle informazioni:
- suppongo che il registro fosse cartaceo e quindi questo ci ricorda che la sicurezza delle informazioni e la privacy non riguardano solo i dati digitali e quindi la cybersecurity, ma anche altri dati;
- in molte organizzazioni i registri degli accessi sono usati male, lasciati in mano alle persone che entrano e senza alcun controllo di quanto scrivono e delle successive uscite; in questi casi sarebbe opportuno riflettere sulla loro reale utilità;
- bisognerebbe riflettere sui tempi di conservazione anche per dati di questo tipo.

****

EONL