Cesare Gallotti

****
IT SERVICE MANAGEMENT NEWS – APRILE 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

PRIMA PARTE: TUTTO IL RESTO
01- Stato delle norme ISO/IEC 270xx - Aprile 2018
02- Nuova ISO/IEC 17025 sui laboratori
03- Direttiva NIS in vigore (ma non troppo)
04- Nuova versione del NIST Cyber Security Framework
05- Come è (im)possibile dimostrare che il proprio pc è stato compromesso

SECONDA PARTE: GDPR (manca una settimana...)
06- 24 maggio: incontro del Garante
07- Traduzione ENISA handbook
08- Linee guida WP art. 29 su consenso e trasparenza
09- GDPR: La mia lista
10- GDPR: qualche orrore
11- Ius law web radio: Come stabilire le misure di sicurezza con la ISO/IEC 29151
12- GDPR: Valutazione del rischio e PIA
13- GDPR: Perché avere un DPO certificato
14- GDPR: Casi pratici sui fornitori
15- Le non-deroghe alle sanzioni sul GDPR
16- GDPR: Deroga sul registro dei trattamenti

****
PRIMA PARTE: TUTTO IL RESTO

01- Stato delle norme ISO/IEC 270xx - Aprile 2018

Il 20 aprile a Wuhan (Cina) si è concluso l'incontro semestrale del ISO/IEC JTC 1 SC 27, ossia del comitato che si occupa della redazione delle norme della serie ISO/IEC 27000.

Ho trovato l'incontro povero di argomenti di mio interesse. Darò quindi conto delle (poche) cose emerse.

Per quanto riguarda i lavori sulle norme della privacy, i lavori sulla ISO/IEC 27552 (ossia lo standard che potrebbe essere quello su cui sarà basata la "certificazione GDPR") sono proseguiti e verrà prodotto un secondo CD. In parole molto povere: i lavori stanno proseguendo come previsto in precedenza, con pubblicazione della norma prevista a fine 2019.

Altra norma che è ritenuta molto interessante è la ISO/IEC 27018 (Code of practice for PII protection in public clouds acting as PII processors). E' programmata una sua nuova versione a breve per allinearla alle altre norme uscite in questi anni. Purtroppo mi risulta non siano state fatte riflessioni approfondite sulle sovrapposizioni tra questa norma e la ISO/IEC 27552.

Altri lavori sono proseguiti (ma non ho potuto seguirli perché arrivato tardi per problemi vari). In particolare sulla nuova edizione della ISO/IEC 29101 (Privacy Architecture Framework) e la ISO/IEC 27550 (Privacy engineering for system life cycle processes).

Lascio in coda le attività del WG 1, ossia quelle più strettamente collegate alla ISO/IEC 27001. Segnalo le cose per me più interessanti:
- c'è stato un incontro di discussione sulla "utilità del SOA", in cui sono emersi i diversi punti di vista;
- sono continuati i lavori preparatori per la prossima versione della ISO/IEC 27002;
- sono continuate le discussioni per la futura ISO/IEC 27005;
- sono state fatte alcune riflessioni sulla ISO/IEC 27006 perché alcuni punti sono risultati ambigui;

Stanno inoltre avanzando i lavori su alcune norme relative alla cybersecurity. In particolare, anche se non ci ho partecipato, trovo molto interessante la futura norma ISO/IEC 27102 sulle cyber-assicurazioni.

Per quanto riguarda i partecipanti, ho solo i numeri del WG 1 (i gruppi sono 5 e il WG 1 è il più numeroso): 98 esperti da 21 Paesi. La delegazione italiana (per i soli WG 1 e WG 5) era composta da ben (!) tre persone.

PS: la versione in inglese di questo articolo: https://www.linkedin.com/pulse/isoiec-27xxx-standards-update-cesare-gallotti.

****

02- Nuova ISO/IEC 17025 sui laboratori

E' stata pubblicata la versione del 2017 della ISO/IEC 17025, applicabile ai laboratori:
- https://www.iso.org/standard/66912.html.

La notizia l'avevo sottovalutata, ma in realtà essa ha impatto sui "laboratori" che conducono vulnerability assessment e penetration test (da ricordare che AgID, per l'applicazione del Regolamento eIDAS, richiede che i tali laboratori siano accreditati ISO/IEC 17025 entro il 1 giugno 2019) e sui laboratori di acquisizione e analisi delle prove forensi.

Per questo segnalo questo articolo di Forensics Focus che fornisce dettagli sulle novità della ISO/IEC 17025:
- https://articles.forensicfocus.com/2018/04/20/changes-to-forensic-laboratory-accreditation-requirements-iso-iec-17025/.

****

03- Direttiva NIS in vigore (ma non troppo)

La newsletter SANS Newsbites mi ha ricordato che il 10 maggio sarebbe dovuta entrare in vigore la Direttiva NIS (Networks and Information Systems).

In altre parole, i Paesi membri avrebbero dovuto approvare entro il 10 maggio una normativa nazionale (in Italia, un Decreto Legislativo) di recepimento della Direttiva. Non mi risulta che l'Italia l'abbia ancora fatto, anche se il Governo ha avuto la delega ad ottobre 2017 (ma sappiamo bene cose è successo nel nostro Paese da ottobre ad oggi).

La Direttiva riguarda gli adempimenti che alcuni erogatori di servizi essenziali (per esempio fornitura di elettricità, acqua, servizi sanitari e di trasporto passeggeri e merci) dovrebbero attuare per assicurare la sicurezza dei propri sistemi informatici.

Finita la sbornia da GDPR, molto dopo il 25 maggio, immagino, ci accorgeremo anche di questo adempimento.

Intanto possiamo studiarci la materia grazie agli... inglesi! Il National Cyber Security Centre ha infatti pubblicato una guida alla NIS:
- https://www.ncsc.gov.uk/guidance/nis-guidance-collection.

(Confesso che non ho capito se l'UK ha approvato un proprio provvedimento legislativo nazionale per recepire la Direttiva NIS, ma forse questo non è così importante).

****

04- Nuova versione del NIST Cyber Security Framework

Il NIST ha pubblicato la versione 1.1 del suo "Framework for Improving Critical Infrastructure Cybersecurity", più noto come "Cyber Security Framework" o CSF:
- https://www.nist.gov/cyberframework.

Ho sempre espresso qualche perplessità su alcuni punti del CSF e sul suo uso in alcuni contesti, ma la sua validità è innegabile.

I controlli cambiati sono quelli relativi all'identificazione e autenticazione e alla gestione delle vulnerabilità. Il pdf ha comunque una tabella con i cambiamenti apportati, non solo ai controlli.

Dalla pagina web, sotto il menu "framework", è possibile scaricare anche l'Excel.

****

05- Come è (im)possibile dimostrare che il proprio pc è stato compromesso

Da Crypto-Gram di maggio 2018: Micah Lee ha provato per 2 anni a trovare un metodo per verificare se il proprio pc portatile è stato compromesso. I risultati lasciano dei dubbi e dimostrano quanto sia difficile verificare la compromissione di un pc portatile:
- https://theintercept.com/2018/04/28/computer-malware-tampering/.

Ancora una volta trovo conferma dell'impossibilità di avere certe misurazioni della sicurezza e valutazioni del rischio quantitative.

****

SECONDA PARTE: GDPR (manca una settimana...)

06- 24 maggio: incontro del Garante

Il 24 maggio a Bologna è stato organizzato l'evento "Regolamento Ue. Il Garante incontra i Responsabili della Protezione dei Dati (RPD)":
- http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7917099.

Io, grazie al solito Pierfrancesco Maistrello, mi ero iscritto per tempo.

Per chi fosse interessato, l'evento può essere seguito in streaming come riportato dalla pagina sopra indicata.

****

07- Traduzione ENISA handbook

Franco Vincenzo Ferrari di DNV GL Business Assurance mi ha segnalato la disponibilità di una traduzione in italiano dell'handbook di ENISA:
https://www.amazon.it/clouddrive/share/ikQmbrXD7J6X2WlRXfqdXa3Cs10Mo2EqQlom5oWeUre?_encoding=UTF8&%2AVersion%2A=1&%2Aentries%2A=0&mgh=1.

Credo sia noto il mio apprezzamento per questa pubblicazione (anche se rileggendola con attenzione ho trovato qualche controllo che risente di un'impostazione teorica da torre di cristallo, ma si tratta di pochissimi casi).

Devo dire che il mio ego ha subito un tracollo: alcuni traduttori (con cui mi complimento) li conosco bene, ma non è da loro che mi è arrivata la notizia.

****

08- Linee guida WP art. 29 su consenso e trasparenza

Confesso che leggo raramente le linee guida del WP Art. 29. Infatti solitamente ripetono cose già dette più volte. Lascio ad altri più pazienti (e spesso più competenti) di me il compito di leggerle e identificare eventuali punti originali.

In questo caso Pierfrancesco Maistrello mi è venuto in aiuto con due linee guida.

La prima è sul consenso. La linea guida si trova qui:
- http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051.

Ecco quello che mi scrive Pierfrancesco: "il capitolo 8 riporta una cosa ovvia, anche se ho visto molti casi in cui ovvia non è. Si dice che il consenso raccolto in ambito Direttiva 95/46 (ossia prima del GDPR) può essere valido, previa verifica delle caratteristiche della sua acquisizione. Io direi che se un titolare italiano ha disposto testi informativi conformi con la vigente legge dell'epoca, dovrebbe aver indicato le finalità in informativa e, conseguentemente, agganciato un consenso liberamente selezionabile (e firmabile in caso di trattamento di dati sensibili). Chi invece ha fatto il furbo dovrà correre ai ripari. Molto spesso i contatti del marketing sono stati raccolti nei modi più vari e oggi non è più possibile sapere se erano anche corretti".

Io aggiungo che molti uffici marketing mi chiedono perché non giudicare validi i contatti che hanno ricevuto email promozionali gli scorsi anni e non hanno mai seguito la (semplice) procedure di cancellazione. Non saprei rispondere in modo più intelligente di "se non avete prova del consenso prestato con un'azione "positiva", quel contatto dovreste cancellarlo".

La seconda pubblicazione è sulla trasparenza. Si trova a questo link:
- http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227.

Pierfrancesco mi segnala: "anche qui niente di nuovissimo, mi pare, almeno per chi si è letto il GDPR. In realtà sarebbe importante leggere tutto il documentone, che parte descrivendo l'importanza del primo tassello (cosa che io dico sempre): l'informativa deve essere comprensibile a chi la legge in relazione ai dati che riguardano proprio lui….ma so che è inutile parlarne a te, che la pensi esattamente così da sempre, mi pare…".

Ha ragione a dire che la penso così da sempre. Dubito però di essere stato capace di scrivere un'informativa facilmente comprensibile al cosiddetto "uomo della strada". Ma potrò imparare.

PS: ringrazio ulteriormente Pierfrancesco perché negli ultimi giorni i suoi riassunti mi sono tornati utilissimi.

****

09- GDPR: La mia lista

Fioccano in questi giorni le liste delle cose da fare per il GDPR.

Oggi vedo che finalmente in molti stanno "abbassando i toni", come in questo articolo (segnalatomi da Franco Vincenzo Ferrari):
- https://www.ilfattoquotidiano.it/2018/05/02/nuovo-regolamento-privacy-i-dieci-comandamenti-per-non-cadere-nei-tranelli/4328293/.

Io l'avevo detto nel maggio 2016:
- http://blog.cesaregallotti.it/2016/05/pubblicato-il-nuovo-regolamento-privacy.html.

Ma non avevo considerato la vera grande novità del GDPR: le sanzioni milionarie. Questa è la vera grande novità. Il resto sono solo isterie di "studiosi" o "consulenti" che vogliono vendere mega progetti ai clienti spaventati (o che non hanno capito niente... gli studiosi e i consulenti... non i clienti).

A dirla tutta: il GDPR semplifica di molto rispetto alla 196.

A chi interessa, ecco la mia check list delle cose da fare:

- nei casi previsti dall'articolo 37, designare un DPO; in tutti gli altri casi, individuare un "referente privacy" (anche se non obbligatorio); tutte le altre cose vanno fatte con questa persona (ed eventualmente con altre);
- fare il registro dei trattamenti (il mio modello è il VERA privacy, reperibile da http://www.cesaregallotti.it/Pubblicazioni.html); nessuno chiede di scrivere tanti dettagli, ma di riportare solo i trattamenti e le finalità (e altri dettagli, come richiesto dall'articolo);
- fare una valutazione del rischio relativa alla privacy (si può sempre usare il VERA privacy per iniziare);
- nei casi previsti dall'articolo 35 e dei trattamenti più "rischiosi", fare una valutazione del rischio specifica per quei trattamenti (DPIA o PIA; sempre con il VERA privacy, per iniziare);
- riesaminare l'applicazione territoriale;
- aggiornare le informative, includendo i tempi di conservazione, le modalità di reclamo e, soprattutto, le nuove basi legali (articolo 6 paragrafo 1 del GDPR); togliere anche i riferimenti precisi alla normativa (non servono a niente);
- togliere i consensi non più necessari e documentare (firme non necessarie) quelli necessari (non necessario richiederlo nuovamente); rendere chiaro e "separato" il consenso privacy;
- verificare che gli interessati possano revocare il consenso "con la stessa facilità con cui è accordato";
- ricordare che il GDPR richiede di rispondere alle richieste degli interessati entro un mese (meglio documentare un processo);
- riesaminare tutti i contratti con i fornitori a cui si trasmettono dati personali e, se necessario, aggiornarli (questo è l'adempimento non tecnologico più pesante) con quanto previsto dall'articolo 28 (avevo già preparato una lista dei punti da prevedere a inizio 2017; oggi penso che dovrei modificarla solo lievemente: http://blog.cesaregallotti.it/2017/01/gdpr-e-nomina-dei-responsabili-privacy.html); da prestare attenzione ai fornitori che trasferiscono dati in Paesi extra-UE (in questi casi, applicare quanto previsto dagli articolo 44 e successivi, che consolidano cose già previste dalla precedente normativa);
- riesaminare e, se necessario, aggiornare gli accordi con i con-titolari (ricordando anche qui di prestare attenzione ai trasferimenti extra-UE);
- documentare, per esempio in un mansionario, quali trattamenti sono autorizzati a svolgere le aree aziendali (questo sarebbe un raffinamento di quanto riportato nel registro);
- stabilire un processo di riesame periodico delle autorizzazioni assegnate per accedere ai dati personali (processo già previsto dalle misure minime del D. Lgs. 196, ma ora ancora più importante perché "sostituisce" le nomine agli incaricati insieme al punto precedente);
- predisporre un regolamento privacy (che può anche essere esteso alla sicurezza delle informazioni) per tutto il personale e i collaboratori autorizzati a trattare i dati personali, con misure "generali" e, se il caso, con misure specifiche per alcuni trattamenti (p.e. manutenzione software, gestione contatti di un contact centre);
- stabilire un processo di gestione degli incidenti con impatto sui dati personali (data breach, articoli 33 e 34);
- controllare che i dati possano essere forniti agli interessati in "formato portabile"; nella maggior parte dei casi vuol dire prevedere l'esportazione in un formato strutturato, di uso comune e leggibile da dispositivo automatico (ossia un testo ASCII, una tabella csv o un pdf); in alcuni specifici mercati è invece necessario prevedere altre soluzioni;
- prevedere la cancellazione dei dati quando è terminato il periodo di conservazione, ricordando che il principio della conservazione perché "non si sa mai" non è incluso nel GDPR, anzi... è sanzionato; questo è sicuramente l'adempimento tecnico più pesante;

- stabilire un processo di audit interni per la privacy (testare, verificare e valutare).

PS: la versione in inglese di questo articolo: https://www.linkedin.com/pulse/gdpr-my-list-cesare-gallotti/.

****

10- GDPR: qualche orrore

A pochi giorni dall'entrata in vigore del GDPR, ovviamente le organizzazioni si stanno attrezzando (tantissime hanno aspettato l'ultimo mese!).

Gli orrori quindi si cominciano a vedere e si diffondono, dimostrando così quanto l'eccesso di entusiasmo o di isteria degli ultimi mesi o anni non abbiano fatto sempre bene. Molti esempi vengono anche da grandissime multinazionali, che evidentemente si sono affidate a consulenti dell'ultimo minuto e che hanno venduto loro soluzioni standard, per quanto sciocche esse siano.

Qui elenco qualche caso.

E alla fine fate come volete... ma non ditemi che la privacy è solo burocrazia inutile. Perché la burocrazia inutile se la sono voluta loro, non l'ha imposta il GDPR!

RAPPORTI CON I DIPENDENTI
Sono venuto a conoscenza di una nuova formula di "nomina ad incaricato". Visto che il GDPR non prevede "nomine" o "designazioni", qualcuno non ha voluto rinunciare (anche se poteva farlo sin dal Dlgs 196) al foglio di carta firmato singolarmente dal dipendente e gli ha messo il titolo di "designazione a persona autorizzata al trattamento dei dati personali".

La firma è anche richiesta quando sono inviate al personale le regole da seguire per assicurare la protezione dei dati personali. Io sono un promotore di tale regolamento, ma perché richiedere la firma per accettazione, quando per tutte le altre regole e procedure aziendali non è richiesta alcuna firma? Perché introdurre un processo "diverso"?

Ovviamente, è sempre in voga la richiesta di firma sull'informativa, anche se non richiesta. Alcuni, ahinoi, continuano anche a richiedere il consenso.

Credo che i dipendenti, in tutta la loro vita lavorativa, con l'eccezione del contratto di assunzione, firmino solo i documenti di "autorizzazione al trattamento dei dati personali", "regolamento per la protezione dei dati personali" e "informativa relativa al trattamento dei dati personali". Firma autografa, visto che siamo nel 2018...

GESTIONE DEI FORNITORI
Si stanno diffondendo i questionari ai fornitori. Ma il GDPR non li richiede. Il GDPR richiede di stipulare contratti che impongano ai fornitori (responsabili del trattamento) l'attuazione di misure di sicurezza che il titolare ritiene adeguate.

Qualcuno mi dice che questi questionari servono a valutare il rischio del fornitore. Purtroppo è un'interpretazione sbagliata: il titolare deve valutare il rischio dei trattamenti, stabilire le misure "adeguate" e poi richiederne l'attuazione ai fornitori. Processo più logico di quello di inviare il questionario, poi valutare il rischio, poi stabilire se il fornitore è adeguato, poi... poi cosa?

Se il fornitore non può accettare le clausole contrattuali, avvierà una negoziazione con il cliente, proponendo misure compensative, segnalando quelle non applicabili al trattamento affidato, eccetera. Forse questo è un processo troppo logico...

PS: la versione in inglese è qui: https://www.linkedin.com/pulse/gdpr-doghouse-list-mistkes-cesare-gallotti/

****

11- Ius law web radio: Come stabilire le misure di sicurezza con la ISO/IEC 29151

Elia Barbujani di Ius law web radio mi ha intervistato su misure di sicurezza per la privacy e ISO/IEC 29115. La puntata (35 minuti) è qui:
- https://webradioiuslaw.it/speciale-adeguamento-privacy-come-stabilire-le-misure-di-sicurezza-secondo-la-iso29151/.

****

12- GDPR: Valutazione del rischio e PIA

Segnalo questo mio articolo su ICT Security Magazine dal titolo "Valutazione del rischio e PIA", sulle relazioni e le differenze tra valutazione del rischio relativo alla privacy e PIA:
- https://www.ictsecuritymagazine.com/articoli/valutazione-del-rischio-e-pia/.

****

13- GDPR: Perché avere un DPO certificato

Mi sono sempre chiesto perché tanta fretta ad avere le tanto pubblicizzate certificazioni da DPO.

Franco Ferrari di DNV GL mi ha inoltrato il link a questo articolo che me lo spiega:
- https://www.puntosicuro.it/security-C-124/privacy-C-89/la-qualificazione-dei-responsabili-del-trattamento-della-protezione-dei-dati-AR-18008/.

In sostanza, una persona certificata secondo una norma UNI (in questo caso, DPO secondo quanto previsto dalla norma UNI 11697) garantisce di poter offrire una "prestazione a regola d'arte". Come dice l'articolo: "l'adeguarsi alla norma UNI 11697 è fatto volontario e garantisce che il soggetto conforme a questa norma possa offrire una prestazione a regola d'arte".

Ecco quindi che un titolare, "se sceglie soggetti certificati secondo la norma UNI, per definizione egli non può sbagliare e quindi non è soggetto ad una possibile " culpa in eligendo"".

Segnalo che ora sono ancora in fase di approvazione, da parte di Accredia, i primi accreditamenti alle società che vogliono certificare secondo la UNI 11697.

PS: Monica Perego mi ha chiesto quale sia il documento legislativo che stabilisce come la fornitura di un bene o la prestazione di un servizio, eseguita in conformità a norme UNI, CEI od equivalenti norme europee od internazionali, costituisce fornitura o prestazione a “regola d’arte”. Non le ho saputo rispondere. Se qualcuno ha la risposta, prego di fornirmela.

****

14- GDPR: Casi pratici sui fornitori

In questi giorni molti miei clienti stanno "scoprendo" quanto sia difficile adeguarsi al GDPR quando si tratta di gestire i fornitori, ossia i "responsabili" o "processor".

I casi sono numerosi e normalmente riguarda i grandi fornitori che impongono il proprio modello contrattuale.

Qualche esempio:
- un fornitore ha risposto al mio cliente che non concede il diritto di audit (ma a sua volta se lo prende per verificare se il cliente usa il proprio software senza aver pagato il numero corretto di licenze);
- un grosso fornitore di servizi cloud anche di gestione del personale non prevede la localizzazione dei dati né fornisce alcuna garanzia richiesta dal GDPR (Paese ritenuto adeguato, clausole contrattuali o BCR nel caso di grandi imprese);
- un fornitore non ha voluto specificare le misure di sicurezza adottate.

Cambiare fornitore, lo sappiamo, non è facile. Non solo per questioni economiche dirette (la transizione

sicuramente ha un costo), ma anche perché il rapporto con il precedente fornitore si è consolidato negli anni in termini di condivisione delle procedure e di competenze.

Dovremo aspettare le multe perché finalmente i contratti siano adeguati al GDPR? Temo sarà così.

****

15- Le non-deroghe alle sanzioni sul GDPR

Come è noto, il CNIL (il Garante francese) ha annunciato un periodo "di grazia" per le sanzioni previste dal GDPR per i primi 6 mesi dalla sua entrata in vigore (mi spiace, ma non trovo la notizia corretta, anche se la seguente è chiara):
- https://www.cnil.fr/fr/rgpd-comment-la-cnil-vous-accompagne-dans-cette-periode-transitoire.

Il Garante italiano, a seguito dei rallentamenti sulla "normativa italiana che adegua il Codice privacy al GDPR" ha pubblicato un Provvedimento forse un po' troppo prolisso che, in sostanza, tratta anche dei controlli previsti per il GDPR, ma si conclude dicendo che entrerà in vigore dopo 6 mesi dall'entrata in vigore della "nuova normativa italiana" (grazie a Pierfrancesco Maistrello per la segnalazione):
- http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/8080493.

C'è chi ha voluto leggerci un periodo di 6 mesi di sospensione (da maggio a novembre, quindi) dei controlli relativi all'applicazione del GDPR in Italia (grazie a Luca Gibilterra per la segnalazione):
- https://www.agendadigitale.eu/sicurezza/privacy/gdpr-il-garante-privacy-differisce-di-sei-mesi-i-controlli-su-applicazione/.

Essendo la fonte autorevole (Gabriele Faggioli, non solo persona molto preparata, ma anche Presidente del Clusit), la notizia si è diffusa velocemente e il Garante ha dovuto chiarire la questione (grazie a Pierfrancesco Maistrello):
- http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/8469593.

In effetti, visto che non si sa quando sarà approvata la "normativa italiana", si rischiava di non vedere alcun controllo del Garante per lunghi anni.

Faggioli ha comunque voluto replicare (grazie a Luca Gibilterra per la segnalazione):
- https://www.agendadigitale.eu/sicurezza/privacy/gdpr-ecco-perche-riteniamo-ci-sia-stato-un-rinvio-dei-controlli-sulle-aziende/.

Io sarò semplicistico, ma eviterei di sperare in una deroga delle sanzioni di qualsiasi tipo. Il Garante ha più volte ripetuto che non la promuoverà. Inoltre credo che il Garante non sia l'unico che può indagare e sanzionare a norma del GDPR.

PS: alcuni post italiani non mi sembra siano più disponibili. Ad ogni modo la storia è interessante perché ci illustra quanto crescano aspettative e isteria con l'avvicinarsi del 25 maggio.

****

16- GDPR: Deroga sul registro dei trattamenti

Pierfrancesco Maistrello mi ha segnalato questo Position paper del WP Art. 29, che riguarda le deroghe relative al registro dei trattamenti:
- http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=624045.

Come è noto, il registro dei trattamenti non va fatto dalle organizzazioni con meno di 250 persone che non trattano dati sensibili (ci sono anche altri casi). Ovviamente, risulta ovvio che tutte le aziende con dipendenti tratta dati sensibili, seppure in modo limitato, e quindi l'esclusione risulta un po' ridicola.

Il WP Art. 29 chiarisce questo fatto, per quanto ovvio, ma aggiunge che in questi casi il registro dovrebbe riportare solo i trattamenti non occasionali che presentano rischi per gli interessati, relativi ai dati sensibili o

giudiziari.

Il documento conclude con la "solita" raccomandazione di fare comunque il registro completo. Posso aggiungere dicendo che a questo punto, in effetti, costerebbe veramente poco completarlo con gli altri trattamenti.

Fonti ben informate (!) mi dicono che il nostro Garante vorrebbe proporre di non fare proprio il registro dei trattamenti quando i trattamenti di dati sensibili si riducono a quelli del personale in aziende di meno di 250 persone. Ma pare che gli altri garanti europei non siano d'accordo.

****