Cesare Gallotti

****

IT SERVICE MANAGEMENT NEWS – FEBBRAIO 2017

****

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.

E' possibile iscriversi o dis-iscriversi
- scrivendo a cesaregallotti@cesaregallotti.it
- seguendo le istruzioni riportate nella pagina http://www.cesaregallotti.it/Newsletter.html

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

****

Indice

01- Aggiornamento legislativo
02- Privacy: GDPR e nomina dei responsabili privacy
03- Privacy: Ingiunzione a responsabile del trattamento
04- Privacy: Garante e raccolta dei log di AdS
05- Privacy: Linee guida DPO in Italiano
06- Segreto industriale e misure di protezione
07- Metodi Agile, qualità e sicurezza
08- ENISA Threat Landscape 2016
09- Prodotti di sicurezza insicuri

****

01- Aggiornamento legislativo

Ho caricato una presentazione sulla normativa legale applicabile alle certificazioni ISO 9001 e ISO/IEC 27001 (pdf, 331KB).

La pagina da cui scaricarla:
- http://www.cesaregallotti.it/Pubblicazioni.html.

Il link diretto:
- http://www.cesaregallotti.it/Pdf/Pubblicazioni/2017-Aggiornamento%20legislativo%20al%2020170130.pdf.

****

02- Privacy: GDPR e nomina dei responsabili privacy

Il Regolamento europeo privacy (GDPR) riporta agli articoli 28 e 29 le modalità di nomina dei responsabili (processor) del trattamento. Queste risultano più precise di quelle previste dal Codice privacy. In particolare, richiede che la nomina avvenga attraverso contratto o da altro atto giuridico.

Tale atto deve riportare:
- oggetto delle attività affidate, includendo la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati;
- clausole di riservatezza;
- garanzia di aver stipulato con il personale con accesso ai dati un obbligo di riservatezza;
- divieto di uso di fornitori da parte del responsabile per il trattamento dei dati senza autorizzazione del titolare;
- impegno, in caso di uso autorizzato di fornitori del responsabile, di prevedere un contratto scritto con riportati i medesimi a cui è soggetto il responsabile;
- le regole da seguire nel trattamento dei dati per controllare i rischi di accesso non autorizzato, divulgazione, mancanza di integrità e indisponibilità dei dati, sia accidentali sia illegali;
- divieto, senza previa autorizzazione del titolare, di trasmettere o conservare i dati in Paesi extra-UE o di fornire accesso a tali dati a personale sito in Paesi Extra-UE;
- l'impegno a verificare periodicamente l'efficacia delle misure tecniche e organizzative per garantire la sicurezza del trattamento;
- l'impegno a dare seguito alle richieste avanzate dal titolare o dagli interessati per dare seguito all'esercizio dei diritti degli interessati al trattamento dei dati personali in modo da poter dare loro risposta entro 30 giorni dalla richiesta;
- l'impegno a comunicare al titolare eventuali violazioni ai dati personali trattati e fornire assistenza al titolare nel caso in cui si manifestino tali eventi;
- la cancellazione o restituzione dei dati al termine delle prestazioni;
- il diritto di audit da parte del titolare.

Si tratta di clausole molto impegnative e sembrano più applicabili a responsabili esterni che interni. Questo anche considerando quanto scritto da Gianfranco Butti in un articolo su Europrivacy:
- http://europrivacy.info/it/2016/07/19/the-internal-data-processor-and-the-gdpr/.

Se ci pensiamo attentamente non pare logico prevedere responsabili interni e strutturare un'azienda su solo 3 livelli gerarchici (titolare, responsabile e incaricato). È anche vero che il GDPR consente esplicitamente la nomina di responsabili da parte dei responsabili e questo permetterebbe la strutturazione in più livelli. Dall'altra parte, invece, si può immaginare che in un'azienda i ruoli e le responsabilità vengano distribuiti non in conformità agli articoli 28 e 29, ma secondo la "normale" gerarchia interna. Il GDPR, infatti, usa il termine "processor", difficilmente applicabile ad una persona e facilmente applicabile ad un'impresa.

Altri (libro "Il regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali" di Enrico Pelino, Luca Bolognini, Camilla Bistolfi) confermano questa lettura.

Se letto in questo modo, il GDPR ci imporrebbe un completo ripensamento su come vedere questi concetti.

****

03- Privacy: Ingiunzione a responsabile del trattamento

Pierfrancesco Maistrello, dopo aver letto il mio post in merito ai responsabili del trattamento secondo il GDPR, mi ha segnalato un'ingiunzione a una responsabile interna del trattamento:
- http://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/3039524.

Qui la responsabile ha dovuto pagare 10 mila Euro, sulla base della normativa vigente. Se il fatto fosse avvenuto tra un anno e mezzo (dopo il maggio 2018), ne avrebbe dovuti pagare 10 milioni. Come dice Giancarlo Butti (già citato dall'articolo precedente), chi vorrà accettare una nomina a responsabile?

****

04- Privacy: Garante e raccolta dei log di AdS

A seguito di un breve dibattito via email, Pierfrancesco Maistrello mi ha segnalato un Provvedimento del Garante del 2014:
- http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3438899.

Colpevolmente, non l'avevo mai notato e invece è interessantissimo.

Intanto, perché nel merito chiarisce come sono valutati i sistemi di raccolta dei log: "Pertanto, la registrazione solo in locale degli accessi applicativi degli amministratori di sistema – l'unica disponibile finché la società non ha introdotto le misure tecniche necessarie per registrare su Arcsight anche tali tipi di accessi – non soddisfa i requisiti stabiliti dalla citata prescrizione". In altre parole, un'azienda deve prevedere un sistema di raccolta centralizzata dei log o sistemi più complessi (la raccolta centralizzata dei log con strumenti gratuiti come Splunk mi risulta essere la soluzione più economica).

Inoltre, è interessante osservare la lunga disquisizione su come interpretare le FAQ del Garante stesso. Da parte mia, penso che troppo spesso siano più fonte di confusione che altro e il Garante potrebbe anche evitare di farle.

****

05- Privacy: Linee guida DPO in Italiano

Pierfrancesco Maistrello mi ha segnalato che il Garante ha tradotto in italiano e pubblicato le linee guida sul DPO ("Linee-guida sui responsabili della protezione dei dati (RPD)") del WP Art. 29:
- http://www.garanteprivacy.it/rpd.

****

06- Segreto industriale e misure di protezione

Da Filodiritto segnalo questo articolo dal titolo "Segreto industriale: l'importanza delle misure di protezione":
- http://www.filodiritto.com/articoli/2017/01/segreto-industriale-limportanza-delle-misure-di-protezione.html.

Un ex socio di un'azienda ha usato, per una concorrente, dei progetti preparati per la prima azienda.

La causa successiva ha evidenziato quali misure dovrebbero essere messe in atto da un'azienda per proteggere (e dimostrare di voler proteggere) i propri segreti industriali:
- ricordare ai propri dipendenti e collaboratori della natura delle informazioni e della necessità di mantenere il segreto sia come condizione contrattuale, sia come informazione comunque diretta a collaboratori e dipendenti (art. 98 e 99 del Codice della proprietà industriale, D. Lgs. 30 del 2005);
- predisporre meccanismi per impedire l'accesso ai dati (almeno sotto forma di istruzioni scritte), dove la conservazione su un unico computer personale con accesso controllato da password non pare sufficiente (mentre poteva avere maggiore valore la conservazione su un server "aziendale").

****

07- Metodi Agile, qualità e sicurezza

Ho caricato una presentazione sui metodi Agile e come correlarli ai requisiti delle norme ISO 9001 e ISO/IEC 27001.

La pagina da cui scaricarla:
- http://www.cesaregallotti.it/Pubblicazioni.html.

Il link diretto:
- http://www.cesaregallotti.it/Pdf/Pubblicazioni/2017-Agile-ISO9001-ISOIEC27001.pdf.

****

08- ENISA Threat Landscape 2016

Quest'anno è Fabio Teoldi, che ringrazio, a segnalarmi la nuova versione dell'ENISA Threat Landscape:
- https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016.

Questo rapporto è accompagnato da altri due rapporti più specialistici, uno sull'hardware e uno sulle comunicazioni M2M:
- https://www.enisa.europa.eu/publications/hardware-threat-landscape;
- https://www.enisa.europa.eu/publications/m2m-communications-threat-landscape.

****

09- Prodotti di sicurezza insicuri

Marco Fabbrini mi segnala questo link "a conferma che molti antivirus sono più dannosi che altro":
- http://www.zdnet.com/article/google-and-mozillas-message-to-av-and-security-firms-stop-trashing-https/.

Continuo a copiare quanto mi ha scritto Marco: "Secondo uno studio condotto dai ricercatori di Google, Mozilla, Cloudflare, e di diverse università degli Stati Uniti, un sorprendentemente elevato numero di antivirus e prodotti di sicurezza ficcano il naso nelle connessioni HTTPS ed espongono gli utenti dei browser ad attacchi".

Grazie Marco.