Cesare Gallotti

****
IT SERVICE MANAGEMENT NEWS – LUGLIO 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 è possibile consultare l'informativa sul trattamento dei dati personali.

****
Indice

****
00- Editoriale

Come sempre a luglio, faccio gli auguri di buon agosto a tutti i miei lettori. La newsletter va in vacanza e spero che tutti possiate riposarvi o almeno passare questo mese in tranquillità.

Questo mese è pieno di privacy (ed EDPS), ma le notizie giunte sono queste. E poi c'è anche il librino della prima notizia a cui tengo moltissimo. Però, come sempre, le notizie privacy sono date dopo tutte le altre, anche se il caso Schrem II è importantissimo.

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

Speravo di pubblicare un libro sulla privacy prima della fine di luglio in modo da fornire una lettura per il mare ai più temerari. Purtroppo non ce l'ho fatta.

Il libro non è mio, ma degli Idraulici della privacy, di cui faccio parte. E' partito da una mia idea e io ho l'onere di pubblicarlo materialmente (lo farò su Streetlib, come il mio "Sicurezza delle informazioni"), ma è un prodotto collettivo.

Quindi questo messaggio è una forma di provino, come si chiamavano un tempo.

Il librino non produrrà niente di troppo originale, ma vuole essere decisamente pratico e indicare una strada per applicare il GDPR almeno nei casi più comuni. Io mi sono divertito molto a partecipare perché

ho avuto modo di imparare cose che avevo trascurato o, in alcuni casi, capito male.

Infine, e questa è la cosa più importante, il ricavato andrà tutto in beneficenza. Il libro è nato durante la clausura e questa esperienza ci ha fatto capire che, se possiamo, dobbiamo aiutare chi ne ha bisogno. Non abbiamo ancora deciso a chi, ma lo decideremo tutti insieme.

Quindi: spero di potervi invitare ad acquistare il libro, disponibile in tutti i negozi online, in formato epub e pdf (e forse cartaceo) dai primi di agosto.

****

02- Sugli SLA

Roberto Beneduci di CoreTech mi ha citato in un suo video in cui spiega gli SLA:
- https://www.linkedin.com/comm/feed/update/urn%3Ali%3Aactivity%3A6685576120831623168.

Mi rendo conto che siamo alla pubblicità reciproca (lui cita me, io cito lui; io gli gratto la schiena se lui la gratta a me o, per tirare fuori il latino, do ut des). Però mi piace molto questo approccio di presentazione di servizi e prodotti attraverso la diffusione di conoscenza, segno anche di curiosità personale e di un certo tipo di entusiasmo non comune.

Insomma: è anche pubblicità, ma di quella che a me piace e quindi spudoratamente, per questa volta, mi associo.

****

03- Ancora sulle nuove regole per i servizi fiduciari

Poco tempo fa avevo segnalato un aggiornamento delle regole Accredia sulle certificazioni eIDAS, ossia quelle per i fornitori di servizi fiduciari regolamentati dal Regolamento eIDAS (per esempio di firme digitali e marche temporali).

Sempre a questo proposito segnalo un articolo dal titolo "Firma elettronica, le regole europee e nazionali per la conservazione dei dati", che approfondisce ulteriormente la questione:
- https://www.key4biz.it/firma-elettronica-le-regole-europee-e-nazionali-per-la-conservazione-dei-dati/312300/.

****

04- Nuove Direttive per i consumatori in ambito digitale

Segnalo questo articolo dal titolo "New Deal For Consumers, come prepararsi alle nuove regole":
- https://www.key4biz.it/new-deal-for-consumers-come-prepararsi-alle-nuove-regole/311782/.

Imparo quindi che nel 2019 furono pubblicate due Direttive che a loro volta richiederanno, entro luglio 2021, delle modifiche al Codice del comumo (D. Lgs. 205/2006).

Copio e incollo: "Le direttive fanno parte del cosiddetto "New Deal for Consumers", un insieme di prescrizioni finalizzato a modernizzare le regole di protezione dei consumatori in vista e in funzione della vertiginosa espansione dell'evoluzione digitale, che attraversa l'automazione delle attività e dei processi di business, le catene di approvvigionamento e gli stessi prodotti e servizi".

Questo è un articolo molto di base. Spero di avere l'opportunità di trovare ulteriori articoli più approfonditi.

****

05- Invalidato il Privacy Shield per i trasferimenti dei dati negli USA

Notizia importantissima, è l'invalidamento del Privacy Shield. Per trasferire i dati negli USA (principalmente per usare i grandi fornitori di servizi informatici o di supporto) era ritenuta adeguata l'adesione al Privacy Shield dell'organizzazione ricevente. Nel 2015 era già stato invalidato il protocollo Safe Harbour, predecessore del Privacy Shield.

La sentenza completa della Court of Justice of the European Union del 16 luglio 2020 è qui (grazie a Gianluca Dalla Riva degli Idraulici della privacy):
- https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62018CJ0311.

Il comunicato dell'EDPS conferma l'appoggio alla posizione presa, ma non illumina su cosa fare:
- https://edps.europa.eu/press-publications/press-news/press-releases/2020/edps-statement-following-court-justice-ruling-case_en.

Per capire cosa fare, si possono leggere i comunicati stampa della Corte stessa:
- Italiano: https://curia.europa.eu/jcms/jcms/p1_3117876/en/;
- Inglese: https://curia.europa.eu/jcms/jcms/p1_3117870/en/.

In sostanza: usare le clausole contrattuali tipo, però potrebbe non essere sufficiente.

Pierfrancesco Maistrello mi ha segnalato il sito di Schrems, ossia quello che ha provocato la caduta:
- https://noyb.eu/en/next-steps-eu-companies-faqs.

Qui si pongono molti problemi. Infatti non sembra sia sufficiente usare le SCC o verificare se il fornitore assicura l'uso di server in Europa, perché, essendo società statunitensi, rientrano nel FISA 702 che è una della cause per cui il Privacy Shield è caduto.

Aggiungo che anche i servizi applicativi sono colpiti da questa sentenza: Salesforce, Hubspot, MailChimps, tutte le email su Google, Sharepoint e OneDrive, WeTransfer e così via. E penso che anche i servizi di Zoom, GoToMeeting e compagnia che ci hanno tenuto compagnia durante la clausura siano colpiti. E non tutti questi servizi prevedono la possibilità di essere erogati solo da server europei.

Potrei sempre sbagliarmi.

Su Web Ius Law c'è un podcast con Alessandro Del Ninno:
- https://webradioiuslaw.it/speciale-adeguamento-privacy-tutto-quello-che-volevi-sapere-sulle-clausole-contrattuali-standard/.

Luca Bolognini e Giovanni Ziccardi hanno fatto un podcast di 90 minuti (grazie sempre a Pierfrancesco Maistrello per il link):
- https://zerodays.podbean.com/e/luca-bolognini-spiega-da-zero-il-caso-schrems-ii-e-il-trasferimento-dei-dati-allestero-nel-gdpr/.

Venerdì 24 alle 14 ci sarà un ulteriore podcast sempre con Luca Bolognini e Giovanni Ziccardi (non so come sarà accessibile dopo quella data):
- https://www.istitutoitalianoprivacy.it/2020/07/22/open-webinar-sugli-impatti-della-sentenza-della-corte-di-giustizia-ue-schrems-ii/.

Io purtroppo sono più un lettore che un ascoltatore e quindi non ho approfondito a sufficienza la questione. Spero che:
1- il Garante si esprima in merito per aiutare a capire e agire;
2- qualcuno scriva articoli significativi sulla questione (per il momento non ne ho visti, ma se qualcuno me li segnala gliene sarò grato).

****

06- Privacy: Analisi EDPS sui prodotti e servizi Microsoft

L'EDPS (ossia, semplificando, il DPO delle istituzioni della UE) ha pubblicato un rapporto dal titolo "Outcome of own-initiative investigation into EU institutions' use of Microsoft products and services":
- https://edps.europa.eu/sites/edp/files/publication/20-07-02_edps_euis_microsoft_contract_investigation_en.html.

In fondo è possibile trovare il link al pdf.

In sostanza l'EDPS ha analizzato i contratti con Microsoft e ha trovato molte carenze per quanto riguarda

l'applicazione del GDPR. Le cose più significative, a mio parere, sono:
- possibilità di Microsoft di aggiornare unilateralmente e senza preavviso i termini e le condizioni (addirittura Microsoft agisce come titolare);
- carenza di adeguate calusole sul diritto di audit.

C'è anche altro. Penso che, probabilmente, analisi sugli altri grandi fornitori di informatica (p.e. Amazon o Google) darebbero risultati altrettanto significativi. Rimane quindi da sperare che questo rapporto produrrà significativi miglioramenti in tutti i contratti per prodotti e servizi forniti da questi grandi attori.

Ringrazio Franco Vincenzo Ferrari di DNV GL per avermi segnalato il documento.

Penso che se incrociassimo questa notizia con quella dello Schrem II avremmo ulteriori elementi di criticità nell'uso dei grandi fornitori di servizi informatici statunitensi, visto che tutti, più o meno, prevedono clausole simili.

****

07- Privacy: Linee guida EDPS su titolare, responsabile e contitolare

Ricordavo la pubblicazione di Linee guida su titolare, responsabile e contitolare, ma non riuscivo più a trovarle. Poi ho scoperto il perché: pensavo fossero state pubblicate dall'EDPB o dal precedente WP 29, mentre erano state pubblicate dall'EDPS (ossia, per farla breve, dal DPO delle istituzioni europee).

Il documento ha titolo "EDPS Guidelines on the concepts of controller, processor and joint controllership" e si trova qui (in inglese, francese e tedesco):
- https://edps.europa.eu/data-protection/our-work/publications/guidelines/concepts-controller-processor-and-joint_en.

Inizialmente le avevo ignorate in quanto ovvie. Però poi ci si trova sempre davanti ai "casi particolari" e queste linee guida possono tornare utili.

Ringrazio Glauco Rampogna che le ha (ri)segnalate agli Idraulici della privacy.

****

08- Privacy: Rapporto EDPS sulle DPIA fatte nelle istituzioni europee

Segnalo questo articolo dal titolo "DPIA, ecco come la fanno le istituzioni europee: le best practice nel rapporto dell'EDPS":
- https://www.cybersecurity360.it/legal/privacy-dati-personali/dpia-ecco-come-si-fa-nei-paesi-europei-le-best-practice-nel-report-delledps/.

Il rapporto completo si trova sul sito dell'EDPS:
- https://edps.europa.eu/data-protection/our-work/publications/reports/edps-survey-data-protection-impact-assessments-under_en.

Trovo interessante il fatto che le DPIA siano lunghe mediamente 16 pagine. Mi sembrano poche e ne sono contento, dato che vedo spesso applicato il principio del "più pagine sono, meglio è".

EDPS ha poi analizzato come è recepito il proprio modello di DPIA. Io l'ho riguardato:
- https://edps.europa.eu/data-protection/our-work/publications/guidelines/accountability-ground-provisional-guidance_en.

Devo dire che questa guida è molto orientata all'analisi del rispetto dei principi del GDPR, più che all'analisi del rischio. Comunque da considerare.

****

09- Privacy: organismi di monitoraggio dei codici di condotta

Sandro Sanna mi ha segnalato il fatto che il Garante ha stabilito i requisiti di accreditamento degli organismi di monitoraggio dei codici di condotta:
- https://gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9432569.

Sandro nutre il timore che questi codici di condotta potrebbero poi essere utilizzati malamente come certi certificati.

Io penso che il rigore con cui opereranno gli Odm dipenderà da come il Garante li controllerà. Se sono controllati con superficialità dagli OdM, allora questi codici di condotta saranno applicati malamente.

Il mio timore è che le regole non prevedono un controllo molto significativo degli OdM: mi pare soprattutto di tipo documentale e non c'è alcun impegno in merito alle verifiche che il Garante si propone di fare sul campo, solo possibilità generiche nel caso emergano elementi che richiedono dei controlli. Mi pare anche che manchino regole in merito alla gestione delle non conformità rilevate dal Garante.

Io sono abituato alle regole degli organismi di certificazione dei sistemi di gestione, quindi questo approccio mi lascia perplesso. Ma chissà che invece non sia più efficace.

****

10- Privacy: Guida ENISA sulla pseudonimizzazione

Pubblicata la guida ENISA sulla pseudoanonimizzazione, per chi ancora non la conoscesse. Versione in inglese, italiano e francese (grazie a Nicola Nuti degli Idraulici della privacy):
- https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices.

****

11- Privacy: Registro dei Provvedimenti privacy presi in cooperazione tra autorità

Glauco Rampogna degli Idraulici della privacy ha segnalato la pubblicazione del registro contenente le decisioni prese dalle autorità nazionali di vigilanza con la procedura di cooperazione one-stop-shop (articolo 60 del GDPR):
- https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-article-60-final-decisions_en.

Non è di facilissima consultazione perché le "istruzioni" non sono fornite (dopo un po' però si capisce che "LSA" è la leading supervisory authority", "CSA" sono le "concerned supervisory authority" e così via).

Non mi sembra però siano decisioni significative. Sicuramente è però importante vedere l'applicazione della procedura di cooperazione.

****