Cesare Gallotti

Standard ISO/IEC 270xx; Certificazioni GDPR; privacy; minacce e attacchi; sentenze
****
IT SERVICE MANAGEMENT NEWS – OTTOBRE 2019
****

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- Stato delle norme ISO/IEC 270xx

Venerdì 18 ottobre 2019 si è concluso a Parigi il meeting semestrale del ISO/IEC JTC 1 SC 27, ossia del gruppo che, tra gli altri, si occupa delle norme ISO/IEC 27001 e 27701.

Le persone iscritte erano più di 300 (è difficile fare i conti corretti, visto che molti si sono iscritti a più gruppi di lavoro e non riesco a calcolare correttamente il numero totale).

La delegazione italiana era composta da 4 persone (tra cui Fabio Guasconi, Andrea Caccia e io; ringrazio tutti i delegati per avermi segnalato refusi ed errori nella prima versione di questa nota).

Segue lo stato di alcune norme che ritengo essere le più interessanti in lavorazione.

Per quanto riguarda le norme relative ai sistemi di gestione, ossia quelle trattate dal WG 1:
- ISO/IEC 27001: si è avviata una revisione minore solo per allineare l'Annex A alla nuova ISO/IEC 27002 (non è previsto si modifichino altre parti della norma); si pensa quindi di avere le nuove versioni delle due norme nel 2022;
- ISO/IEC 27002 sui controlli di sicurezza: passa in CD e si prevede che la sua nuova versione sarà pubblicata nel 2022;
- ISO/IEC 27004 sulle misurazioni della sicurezza: è stata approvata la pubblicazione di una correzione (non significativa, se non per quelli particolarmente rigorosi);
- ISO/IEC 27005 sulla gestione del rischio: sono ripartiti i lavori e si spera di concluderli all'inizio del 2022;
- ISO/IEC 27011 sui controlli per gli operatori di TLC: è in fase di revisione e si spera di concluderla per fine 2022;
- ISO/IEC 27013 sui rapporti tra ISO/IEC 27001 e ISO/IEC 20000-1; è in fase di revisione per recepire la nuova versione della ISO/IEC 20000-1 (oltre che le esperienze maturate in questi anni).

E' stata avanzata la proposta di una nuova norma ISO/IEC 27104 dal titolo "Guidelines for cyber insurance". Dovrò cercare di capire perché questa norma oltre alla ISO/IEC 27102.

Credo sia significativo segnalare che sono state discusse le possibili azioni da intraprendere, in termini di chiarimenti e di suggerimenti, in merito alle certificazioni ISO/IEC 27001 che usano i controlli aggiuntivi di norme come le ISO/IEC 27001, 27017, 27018 e 27019.

Per quanto riguarda le certificazioni ISO/IEC 27701 e le relative certificazioni GDPR, rimando all'articolo successivo.

Per quanto riguarda le altre norme relative alla privacy, ossia quelle elaborate dal WG 5, credo che la cosa più interessante sia la norma relativa alla cancellazione dei dati personali, ma solo perché la sta seguendo una rappresentante della delegazione italiana.

Avrei voluto seguire alcune norme più tecniche (quelle relative all'IoT e gestite dal WG 4), ma la bizzarra organizzazione ha fatto sì che fossero trattate a più di mezzora di distanza da quelle del WG 1 e WG 5 e la logistica non mi ha permesso di spostarmi in tempo.

****

02- ISO/IEC 27701 e certificazioni GDPR

Al meeting dell'SC 27 si è votato per l'elaborazione di una qualche norma, simile alla ISO/IEC 27006, per le certificazioni ISO/IEC 27701

Si tratterà di una norma basata sulla ISO/IEC 17021 e pertanto non potrà essere considerata nei termini del GDPR, che richiede di usare la ISO/IEC 17065.

Segnalo che i più critici ad usare la ISO/IEC 17065 come base per questa nuova norma sono stati proprio gli europei. Sicuramente questa contrarietà è dovuta ad una certa volontà di mantenere il rigore tecnico (visto che la ISO/IEC 27701 è uno standard per sistemi di gestione e non per processi). In realtà, pare che il mercato richieda proprio uno schema di certificazione sulla ISO/IEC 27701 come sistema di gestione.

Altri mi hanno spiegato che se ISO farà uno schema di certificazione della ISO/IEC 27701 basato sulla ISO/IEC 17021, non si potrà farne un altro basato sulla ISO/IEC 17065 perché le regole EA lo proibiscono.

Sarebbe possibile fare un nuovo standard, anche uguale alla ISO/IEC 27701, ma con altra numerazione, in modo da pensare ad uno schema basato sulla ISO/IEC 17065.

Io penso (e solo il futuro mi darà ragione o torto) che se partirà la certificazione ISO/IEC 27701 (e credo anche che partirà presto), questa avrà abbastanza successo da rendere inutile ogni altra certificazione, anche se basata sull'art. 42 del GDPR. Ci saranno certamente quelli che ribadiranno continuamente che la certificazione ISO/IEC 27701 non è coerente a quanto richiesto dall'articolo 42 del GDPR, ma nella pratica nessuno ci farà caso (esattamente come nessuno fa caso a me quando dico che cyberspazio non si traduce con "spazio cibernetico", che la "cyber-sicurezza" è in realtà la "sicurezza informatica", che certi inventari degli asset sono inutili, eccetera).

Dall'altra parte, in Europa ci sono un paio di organizzazioni che fanno molto rumore per proporre dei loro schemi proprietari, con accreditamento basato su ISO/IEC 17065. La mancanza di uno schema basato su standard non proprietari è comunque un problema e potrà valere la pena lavorare su alternative "pubbliche" (anche se pubbliche non sono).

Per concludere, segnalo un articolo più tecnico sulla ISO/IEC 27701. Questo, dal titolo "ISO/IEC 27701, la norma internazionale per certificare la protezione dei dati personali", è di Fabio Guasconi e avanza alcuni spunti interessanti (per esempio sull'applicabilità presso le PMI di una norma come la ISO/IEC 27701):
- https://www.ictsecuritymagazine.com/articoli/iso-iec-27701-la-norma-internazionale-per-certificare-la-protezione-dei-dati-personali/.

****
03- VERA 5.0

Ho pubblicato il VERA 5.0 (il mio foglio Excel per un approccio per la valutazione del rischio relativo alla sicurezza delle informazioni):
- http://www.cesaregallotti.it/Pubblicazioni.html.

La novità maggiore è che ho messo nello stesso file le cose per ISO/IEC 27001 e per privacy (ISO/IEC 27701).

Qualche altra modifica dalle persone che mi hanno scritto e suggerito (negli ultimi mesi: Gianluca Dalla Riva, Alessandro Gaspari, Pierfrancesco Maistrello, Arturo Messina, Nicola Nuti, Simona Persi, Chiara Ponti, Stefano Posti, Pierluigi Stefli).

Invito tutti a criticare e a farmi avere critiche e suggerimenti.

****
04- Standard: IEC 62443-4-2 sulla sicurezza dei componenti OT (sicurezza industriale)

Franco Vincenzo Ferrari del DNV GL mi ha suggerito questo articolo dal titolo "Lo standard IEC 62443-4-2 per la cyber security industriale: le linee guida". Ho qualche riserva sull'articolo, in particolare sulla disinvoltura con cui confonde security e safety e sulla sua concentrazione sui dispositivi (mentre la norma è applicabile a 4 tipi di componenti), però alcune cose sono decisamente interessanti e ne raccomando la lettura:
- https://www.cybersecurity360.it/legal/lo-standard-iec-62443-4-2-per-la-cyber-security-industriale-le-linee-guida/.

Questa norma riporta i requisiti da considerare per i componenti dei sistemi informatici industriali. I componenti possono essere:
- applicaizoni software;
- dispositivi integrati (Embedded device; dispositivi specifici, incluse PLC e sensori);
- pc o server generici;

- componenti di rete.

I requisiti possono poi essere usati per 4 livelli di sicurezza.

La lettura non è semplice e richiede anche di essere accompagnata dalla IEC 62443-3-3. Allo stato attuale, però, sono convinto che le IEC 62443 rappresentino la lettura allo stato dell'arte in materia di sicurezza informatica industriale (o "OT cyber security", dove però il termine "OT" non è mai usato dalle 62443).

La pagina ufficiale della norma è:
- https://webstore.iec.ch/publication/34421.

****
05- NIST: Cybersecurity per le aziende manifatturiere

Il NIST ha pubblicato un documento dal titolo "NISTIR 8183A, Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide":
- https://csrc.nist.gov/publications/detail/nistir/8183/final.

E' un malloppo di più di 700 pagine divise in 3 documenti.

Il primo è abbastanza generico: riporta le "solite" misure di sicurezza, senza spiegarne bene gli impatti in ambito industriale (o ICS). Però si cela una piccola sorpresa, scritta in piccolo e nelle tabelle di correlazione con le funzionalità. Infatti, per ogni misura del NIST Cybersecurity framework si leggono degli strumenti per attuare la misura indicata.

Il secondo volume presenta esempi di documenti e strumenti per le aziende manifatturiere in serie, mentre il terzo è dedicato alle aziende manifatturiere di singoli prodotti (la terminologia usata dal NIST è "di processo" e "discrete"). Qui le sorprese e le indicazioni sono tante.

Intanto i modelli di documento. Ci sono modelli per le politiche, per le procedure operative (tutte accorpate in un unico documento), per la valutazione del rischio, per la gestione degli incidenti, per il ripristino e per i contratti con i fornitori.

Non tutto condivido (per esempio l'accorpamento di tutte le procedure operative in un unico documento e l'eccessivo livello di dettaglio suggerito; per esempio anche il modello di valutazione del rischio, che non permette di rilevarne l'utilità, visto che è troppo dedicato al calcolo e non all'uso). Altri sicuramente non condivideranno altre cose. Ma penso che il livello di dettaglio sia né troppo né troppo poco e lascia ampio spazio alla personalizzazione da parte degli utilizzatori. Ritengo notevole lo sforzo fatto da una fonte così autorevole.

Al capitolo 4 si trova un elenco, con descrizione e commenti (e con anche suggerimenti per l'installazione e la configurazione), di strumenti tecnologici per attuare alcune misure. L'elenco include strumenti per la rilevazione dei dispositivi (discovery dell'hardware), per la valutazione del rischio, per il backup, per la raccolta e analisi dei log, per i vulnerability assessment, per i ticket di gestione degli incidenti, di data loss prevention, per la cancellazione sicura. Alcuni sono free, altri sono a pagamento. In tutti i casi, un'utile punto di riferimento.

****
06- Minacce e attacchi: Istruzioni in caso di attacco ransomware

Un mio amico è stato colpito dal ransomware NESA. Ho chiesto aiuto a Glauco Rampogna, soprattutto per orientarmi nella marea di articoli e strumenti disponibili.

Mi sembra giusto condividere (anche per ricordarmene) la sua risposta.

"Se l'intenzione è di rimuovere il ransomware, ci sono molti tool (io uso Malwarebytes), ma per decifrare i files purtroppo non posso esserti di aiuto immediato, a quanto pare non è stata ancora trovata la chiave di Nesa.

Nesa è una variante del Ransomware DJVU/STOP su cui i ricercatori stanno lavorando:
- https://www.bleepingcomputer.com/forums/t/671473/stop-ransomware-stop-puma-djvu-promo-drume-help-support-topic/?p=4442422.

Per recuperare i file, o si hanno copie di backup o shadow, oppure è necessario salvare tutti i files cifrati e attendere la decifratura. Alcuni siti sono aggiornati con le varianti decifrate. Ad esempio:
- https://www.nomoreransom.org/;
- https://noransom.kaspersky.com/.

Per verificare se è uno scherzo (quindi si vedono i file con estensione .nesa, ma in realtà un altro cryptolocker), si possono inviare due campioni su questi siti:
- https://www.nomoreransom.org/crypto-sheriff.php;
- https://id-ransomware.malwarehunterteam.com/index.php".

Non mi resta che ringraziare Glauco.

PS: un altro mio amico mi ha scritto che qualcuno potrebbe pensare che il "mio amico" sono in realtà io. Non è così. Ricordo che in quel caso si dice "mio cugino", non "mio amico".

****
07- Minacce e attacchi: Frode con imitazione (con AI) della voce del CEO

Il Wall Street Journal racconta di una frode perpetrata utilizzando un simulatore di voce (basato su AI) di un CEO di un'azienda. La frode è costata all'azienda 243 mila dollari:
- https://thenextweb.com/security/2019/09/02/fraudsters-deepfake-ceos-voice-to-trick-manager-into-transferring-243000/.

Io penso che ci sia qualcosa di sbagliato se un'azienda fa un bonifico sulla base di un'autorizzazione data al telefono. Qui sembra che il finto CEO abbia segnalato la necessità di rimborsare un fornitore, ma chi ha fatto il bonifico vero e proprio avrebbe dovuto ricevere anche una fattura o simile.

Se ho capito bene il caso, è il classico caso in cui la tecnologia è solo la ciliegina sulla torta di uno sfruttamento di altre e meno tecnologiche vulnerabilità.

****
08- Articolo sulle assicurazioni IT (da Bruce Schneier)

Su Crypto-gram di settembre 2019 è stato segnalato un articolo dal titolo "Does insurance have a future in governing cybersecurity?". Segnalo il post di Crypto-gram, che ne propone un estratto:
- https://www.schneier.com/blog/archives/2019/09/on_cybersecurit.html.

Faccio un estratto dell'estratto le assicurazioni sono una forma debole di trattamento del rischio perché:
- gli assicuratori, al momento, si concentrano troppo sulle procedure organizzative e troppo poco su quelle tecnologiche;
- gli assicuratori, anzi, richiedono procedure di base e non offrono incentivi reali per investire in sicurezza;
- coprono i costi di risposta agli incidenti (spesso attraverso servizi esterni), ma si tratta di misure post-incidente, meno utili di quelle di mitigazione preventiva (questo anche perché i costi del recupero sono più facili da quantificare).

D'altra parte, dice sempre l'articolo, degli approcci rigorosi e standard migliorerebbero la sicurezza dei clienti. Tali approcci, però, si baserebbero su misure che poi sarebbero soggette alla legge di Goodhart

("quando una misura diventa un obiettivo cessa di essere una buona misura") perché chi deve essere misurato cercherà di migliorare le misure e non di ridurre il rischio.

Io ho sempre avuto dei dubbi sulle assicurazioni di sicurezza IT e qui trovo ulteriori elementi per essere dubbioso.

Mi piace anche il fatto che si sottolinea il fatto che le misure di prevenzione dovrebbero essere preferite a quelle di recupero (e io aggiungo: anche a quelle di monitoraggio).

****

09- Normativa. Note spese: dematerializzazione e conservazione elettronica

In materia di dematerializzazione delle note spese, Luca De Grazia mi ha segnalato la risposta dell'Agenzia delle Entrate numero 388 del 20 settembre 2019. Le risposte della AE si trovano qui:
- https://www.agenziaentrate.gov.it/portale/web/guest/normativa-e-prassi/risposte-agli-interpelli/interpelli.

Un sunto si trova qui:
- https://www.edotto.com/articolo/note-spese-trasfertisti-possibile-la-conservazione-elettronica.

Mi pare di capire, insomma, che venga richiesto un sistema di conservazione.

Però... ho trovato un articolo più critico e mi pare corretto consultarlo:
- https://www.studiofailla.com/note-spese-digitali-e-fisco/.

Un articolo su una precedente risposta dell'Agenzia delle Entrate si trova qui:
- https://www.leggioggi.it/2017/07/31/note-spese-conservazione-diventa-anche-solo-elettronica/.

Mi pare utile seguire questo tema, in quanto stabilisce le basi della conservazione dei documenti, non solo delle note spese.

****

10- Mio articolo: I rischi della percezione

Ho scritto questo articolo dal titolo "I rischi della percezione":
- https://www.safetysecuritymagazine.com/articoli/i-rischi-della-percezione/.

Si tratta di alcune riflessioni nate leggendo un libro molto interessante.

****

11- Normativa: Perimetro di sicurezza nazionale cibernetica

Premetto che mi piacerebbe essere contraddetto rispetto a quello che qui scrivo.

E' stato approvato il Decreto Legge 105 del 2019 con titolo "Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica", noto anche come il decreto sul "Perimetro di sicurezza nazionale cibernetica":
- www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legge:2019-09-21;105!vig=

Ricordo che si tratta di un Decreto Legge e pertanto dovrebbe essere convertito in Legge entro 3 mesi. La conversione potrebbe avvenire con modifiche o non avvenire proprio. E' pertanto necessario prestare le dovute cautele (e magari ristudiare il testo quando sarà definitivo).

Non l'ho letto (anche perché ci sono troppi incroci con altre normative e non vorrei che poi fra 3 mesi questi siano cambiati), ma ho letto con attenzione l'articolo di Stefano Mele:
- https://www.agendadigitale.eu/sicurezza/sicurezza-nazionale-ict-perche-il-decreto-sul-perimetro-fara-

la-differenza/.

Giancarlo Caroti (grazie!) mi ha anche segnalato che ora abbiamo anche la brochure istituzionale:
- https://www.sicurezzanazionale.gov.it/sisr.nsf/archivio-notizie/la-rete-diplomatica-promuove-il-cyber-made-in-italy.html.

Detto questo, il DL era già stato proposto qualche tempo fa (precedente Governo) come DDL. Ora sembra che si voglia imprimere maggiore velocità al tema e quindi si è preferita la strada del DL, in modo da avere la Legge entro 3 mesi.

Il DL prevede siano indicate le entità che costituiscono il "Perimetro di sicurezza nazionale nel cyberspazio", in modo simile a quanto fatto per la Direttiva NIS che richiedeva fossero identificati gli operatori di servizi essenziali (OSE). Qui, evidentemente, si pensa di estendere l'insieme delle organizzazioni significative da un punto di vista informatico (io, poi, non capisco le differenze tra gli OSE e le organizzazioni previste dal "perimetro", ma non credo sia così importante).

A queste organizzazioni, come già fatto per gli OSE, si impone l'attuazione del Framework per la Cybersecurity del CINI, che ho già criticato e che continuo a non considerare come valido riferimento (l'uso del framework del CINI non è esplicitato, ma credo si nasconda tra i riferimenti ad altre normative.

Questo vuol dire che è esteso l'obbligo (anche con pesanti sanzioni) di applicare delle misure "minime" di sicurezza ad un numero maggiore di organizzazioni rispetto a quelle previste dalla Direttive NIS. Per quanto io critichi lo schema del CINI, ritengo che sia un bene.

Si aggiunge un meccanismo di segnalazione di incidenti. Questa ossessione per la segnalazione degli incidenti non la capisco molto bene.
Ricordo che l'obiettivo dovrebbe essere proprio la prevenzione degli attacchi.

Il DL stabilisce un centro di valutazione dei prodotti informatici (il Centro di Valutazione e Certificazione Nazionale, o CVCN, del MiSE), come peraltro già previsto, seppur parzialmente, dal Cybersecurity Act (e di cui vorrei capire le relazioni con il già esistente OCSI, http://www.ocsi.isticom.it/).

Il DL dà la possibilità al Governo di spegnere una rete in caso di grave incidente. Spero di non vedere mai attuata questa opzione.

Infine introduce la golden power in alcuni settori. Questo non è tema su cui posso dirmi competente, ma permetterebbe di orientare alcuni acquisti in modo da evitare interferenze da parte di altre entità (al momento l'attenzione è concentrata sulla possibilità che la Cina, con il monopolio degli apparati 5G, possa spiare le nostre comunicazioni; credo però che questa misura avrà ulteriori e significativi impatti).

Lascio in conclusione una nota formale. Purtroppo sembra che la traduzione pigra di cyber (usato solo come prefisso) con "cibernetica" (che è un'altra cosa) sia diventata la traduzione ufficiale. Queste sono cose che mi lasciano molto sconcertato.

****
12- Normativa commercio elettronico: Marketplace e IVA

Dalla Circolare 8 del 2019 della Borioli & Colombo Associati, Il Drecreto "crescita", DL 34 del 2019, stabilisce nuove misure in merito alle comunicazioni IVA dei cosiddetti marketplace:
- https://www.commercialistatelematico.com/articoli/2019/05/e-commerce-e-decreto-crescita.html.

Io non conosco assolutamente questa materia (conosco solo Maremagnum come marketplace italiano), ma penso che, per il mio lavoro, sia comunque utile tenerla sotto controllo.

****

13- Sentenza: Hacking etico in Italia: archiviazione per divulgazione di vulnerabilità

Luca De Grazia mi ha segnalato questo interessante sentenza:
- https://www.tomshw.it/altro/tribunale-di-catania-archiviazione-per-un-caso-di-hacking-etico/.

Il GIP di Catania ha reputato infondate le accuse nei confronti di un hacker che aveva segnalato le vulnerabilità di un'applicazione. Insomma, sembra sia la prima sentenza in merito alla "divulgazione responsabile" (o "vulnerability disclosure").

****

14- Sentenza: Lo spamming non è (sempre) reato

Luca De Grazia mi ha segnalato questa notizia dal titolo "Lo spamming non è reato. Anche dopo Gdpr":
- http://app.italiaoggi.it/news/lo-spamming-non-e-reato-anche-dopo-gdpr-2393718.

Luca De Grazia mi dice che il concetto del cosiddetto nocumento era da considerare anche in precedenza.

Io dico che, da un punto di vista generale, questa sentenza mi lascia perplesso perché io continuo a pensare che lo spam crei nocumento. Sicuramente, al di là del mio pensiero, credo sia importante considerare questa sentenza. Credo anche che sia importante ricordare che l'articolo 130 (comma 3-bis) del Codice Privacy (D. Lgs. 196 del 2003) ammetto il cosiddetto soft spam.

****

15- Sentenza: Sì al licenziamento per pc aziendale usato per fini personali

Segnalo questo articolo di Altalex dal titolo "Pc aziendale usato per fini personali? Sì al licenziamento in tronco":
- https://www.altalex.com/documents/news/2019/10/02/pc-aziendale-usato-per-fini-personali-si-al-licenziamento-in-tronco.

La Corte di appello di Roma ha confermato il licenziamento di una lavoratrice per aver navigato su Internet troppo frequentemente e per lungo tempo e aver anche importato un ransomware.

La sentenza è interessante (dovremo anche vedere se ci sarà un intervento della Corte di Cassazione, ma dovremo aspettare anni) perché fornisce indicazioni in merito alle indagini ex post anche in mancanza di informative privacy o simili.

****
16- Privacy: Codice di condotta privacy per i sistemi IT per informazioni creditizie

Chiara Ponti degli Idraulici della privacy ha segnalato che è stato pubblicato il "Codice di condotta per i sistemi informativi gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti":
- https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9141941.

Innanzi tutto vedo che stanno uscendo questi codici di condotta previsti dal GDPR. Non mi pare sia stato stabilito un meccanismo per la loro certificazione, ma almeno ci sono e questo è un bene.

Mi pare un po' curioso che vengano pubblicati codici di condotta per la gestione dei sistemi IT in un settore specifico e non più generali. Forse però è questo che il Garante ha avuto come proposta (anche per il rinnovo dei codici preesistenti) e questo può approvare.

Speravo in qualcosa di più interessante, da cui ricavare indicazioni applicabili ad altri ambiti. Invece sono rimasto deluso. Elenco i punti che ho sottolineato:
- come unica misura tecnica precisa, si specifica che "All'atto del ricevimento dei dati, il gestore verifica la loro congruità attraverso controlli di carattere formale e logico"; si richiama nel seguito la necessità di attuare "adeguate misure tecniche ed organizzative" (come da testo del GDPR), ma ancora una volta il Garante si rifiuta entrare nel merito, superando così l'impostazione precedente (quella delle misure minime);
- fanno eccezioni richiami a "modalità di accesso graduale e selettivo", preclusione di "modalità di accesso che permettano interrogazioni di massa o acquisizioni di elenchi di dati personali", verifica periodica degli algoritmi;
- dedica un intero allegato ai tempi di conservazione; forse sono troppo complicati per le finalità della maggior parte delle imprese, però il punto 8 dell'Allegato 2 è applicabile a quasi tutte (tratta dei backup e della conservazione per 10 anni per "difesa di un proprio diritto in sede giudiziaria, amministrativa, arbitrale o di conciliazione (inclusa la fase propedeutica)";
- presenta un esempio di contitolarità (in questo caso tra il gestore e i partecipanti); il Codice presenta alcune clausole (ricorda che i partecipanti accedono con gli strumenti individuati dal gestore e quali persone possono accedere);
- formalmente, il Codice parla di "autonomo titolare", quando alcuni invece dicono di non usare il termine "autonomo" perché il GDPR non lo usa (secondo me, però, l'uso dell'aggettivo rinforza il concetto nel corso della lettura);
- nell'Allegato 3 è presentato un modello di informativa, che ad alcuni potrebbe risultare utile.

****

17- Privacy: Medico competente è titolare

Elia Barbujani degli Idraulici della privacy mi ha segnalato una risposta del Garante ad un quesito in merito al medico competente. Purtroppo non trovo questo documento sul sito del Garante.

Ma, in poche parole, il Garante ritiene che il medico competente debba essere considerato autonomo rispetto al datore di lavoro. Il Garante fa riferimento anche ad un ulteriore Provvedimento, che però non ho trovato altrettanto chiaro e che è del 2016:
- https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/5149198.

Intanto NON ringrazio Elia perché mi costringe a qualche correzione (ehm ehm ehm).

Su questo però voglio riflettere sui numerosi casi per cui un titolare si sente esente da controlli sulla sicurezza quando trasferisce i dati ad altro titolare. In questo caso specifico, già mi vedo i datori di lavoro non chiedere più alcuna garanzia di sicurezza ai medici competenti.

Questo, a mio parere, è un grave errore. Infatti l'interessato non può decidere di quale medico competente avvalersi ed è costretto ad usare quello scelto dal datore di lavoro. A sua volta il datore di lavoro può scegliere il medico competente e quindi ne è (parzialmente) responsabile. In particolare, deve assicurarsi che il medico garantisca un adeguato livello di sicurezza dei dati. Per questo dovrebbe stipulare un contratto con clasole simili a quelle previste dal GDPR per il rapporto tra titolare e responsabile.

****
18- Privacy: Il DPO esterno deve essere dipendente dell'azienda

Il TAR Puglia ha recentemente annullato un incarico a DPO ad una persona giuridica, in quanto il suo referente (persona fisica) non sembrava "appartenere" ad essa.

Su questo Pietro Calorio degli Idraulici della privacy ha scritto un breve ma esaustivo articolo su LinkedIn:
- https://www.linkedin.com/pulse/quando-il-dpo-%25C3%25A8-una-persona-giuridica-soggetto-che-svolge-calorio.

Pietro cita l'articolo di Giovanni Gallus. Eccolo qui:
- https://www.cybersecurity360.it/news/il-dpo-deve-essere-un-dipendente-non-puo-essere-esterno-il-tar-lecce-fa-discutere/.

****
19- UNI/PdR 66:2019 per la certificazione dei professionisti privacy

Chiara Ponti degli Idraulici della privacy mi ha informato che è stata pubblicata la norma UNI/PdR 66 dal Titolo "Raccomandazioni per la valutazione di conformità ai requisiti definiti dalla UNI 11697:2017 "Attività professionali non regolamentate - Profili professionali relativi al trattamento e alla protezione dei dati personali - Requisiti di conoscenza, abilità e competenza"":
- http://store.uni.com/catalogo/index.php/uni-pdr-66-2019.html.

Il comunicato stampa:
http://www.uni.com/index.php?option=com_content&view=article&id=8543%3Atrattamento-e-protezione-dei-dati-personali-ecco-la-uni-pdr-66&catid=171&Itemid=2612.

Non l'ho letta e leggo solo il titolo e mi pare di capire: c'è la UNI 11697 con i requisiti per la certificazione delle figure professionali in materia di privacy e poi queste altre ulteriori raccomandazioni. Secondo me stanno eccedendo in zelo. Ma, ribadisco, lo dico solo leggendo i titoli.

20- Privacy: Conservazione dei dati: criteri e criticità

Segnalo questo articolo di Monica Perego e Chiara Ponti dal titolo "Conservazione dei dati: criteri e criticità (nell'incertezza normativa)":
- https://www.agendadigitale.eu/sicurezza/privacy/conservazione-dei-dati-criteri-e-criticita-nellincertezza-normativa/.

Monica e Chiara sono due amiche, ma sono soprattutto, a mio parere, molto competenti.

L'articolo è interessante, anche se non condivido con loro la necessità di chiedere al Garante indicazioni "ufficiali": penso che siamo abbastanza grandi per trovare da soli la risposta sui tempi di conservazione.