I MANUALI DELLA PRIVACY

Stefano Gorla, Michele Iaselli, Giuseppe Tacconi
Prefazione a cura di Gianluca De Vincentiis

GLI AUDIT PRIVACY

SECONDO IL NUOVO REGOLAMENTO EUROPEO GDPR 2016/679

Guida pratica per la verifica della protezione dei dati

ITER®

Gli audit privacy secondo il nuovo Regolamento Europeo GDPR 2016/679

Di Stefano Gorla, Michele Iaselli, Giuseppe Tacconi
Prefazione a cura di Gianluca De Vincentiis

Editore
ITER Srl – Milano
Via A. Sacchini, 20
20131 Milano (MI)
www.iter.it

Con il patrocinio di ANDIP - Associazione Nazionale per la Difesa della Privacy

ISBN 978-88-903419-3-9

Stampa
Digital Book s.r.l.
Via Karl Marx, 9
06012 Cerbara - Città di Castello (PG)

Prima edizione settembre 2017

Gli audit privacy secondo il nuovo Regolamento Europeo GDPR 2016/679

Guida pratica per la verifica della protezione dei dati

Indice

1. Prefazione (Gianluca De Vincentiis) 7

2. L'attività di audit dal punto di vista giuridico: rapporti con il GDPR (Michele Iaselli) 11
2.1 Audit e GDPR: introduzione 11
2.2 Cosa si intende per rischio informatico 13
2.3 La sicurezza informatica 16
2.4 Le misure di sicurezza nel codice della privacy e nel Regolamento europeo sulla protezione dei dati personali 20
2.5 Ulteriori regole ed adempimenti del GDPR di rilievo per l'attività di audit 23
2.5.1 Principi da applicare al trattamento dei dati personali 24
2.5.2 Informativa e consenso 26
2.5.3 Diritto di accesso dell'interessato 30
2.5.4 Il diritto di opposizione 31
2.5.5 Diritto alla portabilità 32
2.5.6 Data Breach 34
2.5.7 La valutazione d'impatto sulla protezione dei dati (DPIA) 36
2.5.8 Registri delle attività di trattamento 41
2.5.9 Consultazione preventiva 43
2.6 Conclusioni 43

3. Audit nei sistemi di gestione privacy (Stefano Gorla) 46
3.1 Definizione di audit 46
3.2 L'azienda come sistema 48
3.3 Le normative di riferimento 52
3.4 La figura dell'auditor: competenze 56
3.5 Come svolgere un audit privacy 60
3.6 Cosa controllare 63
3.7 Le fasi dall'audit 65

3.8 Rappresentazione dei risultati dell'audit 73
3.9 Esempio di rapporto privacy 78
3.10 Un modello matematico-statistico per il Sistema Gestione Privacy 82

4. Audit privacy dal punto di vista tecnico-informatico (Giuseppe Tacconi) 88
4.1 Premessa 88
4.2 Quali sono le informazioni che sono oggetto della nostra attenzione 89
4.3 Qual è il livello di riservatezza delle informazioni e come devono essere protette in ambito privacy 91
4.4 Quali sono i vincoli cogenti e/o contrattuali che influiscono sul livello di protezione 92
4.5 Quali sono i workflow aziendali ed i flussi informativi che veicolano le informazioni all'interno e all'esterno dell'organizzazione? 93
4.6 Quali sono le infrastrutture che ospitano le nostre informazioni e come vengono gestite dal punto di vista informatico? 96
4.7 Le protezioni al contorno 102
4.7.1 Il firewall questo sconosciuto 102
4.7.2 Antivirus, malware e altri agenti patogeni 103
4.7.3 Log: tracce nel deserto 105
4.8 Case Study 107

Gli autori 111

1. Prefazione (Gianluca De Vincentiis)

Cos'hanno in comune tra loro le parole Privacy ed Audit? E come mai persone di estrazione professionale diversa si sono ritrovate a scrivere un libro in comune?

Sono queste le prime domande che mi sono posto quando gli autori di questo libro mi hanno chiesto la cortesia di un'opinione ed una introduzione al loro lavoro. Tre professionisti affermati nel loro ambito con i quali ho avuto il piacere ed il vantaggio di lavorare, vederli all'opera e di sviluppare anche un'amicizia personale.

La mia formazione professionale mi porta ad associare immediatamente la parola *Privacy* al complesso delle norme che regolano la tutela e l'utilizzo dei dati personali, mentre la parola *Audit*, sempre nella mia esperienza, risulta essere l'attività (intervista) tesa alla raccolta di evidenze oggettive per una valutazione indipendente e quanto più obiettiva di conformità ad una regola nota e condivisa, tra chi conduce l'audit e chi deve fornire i riscontri richiesti.

Mentre leggevo il testo altre domande si aggiungevano alle prime, ed in particolare una è rimasta sempre latente sino alla fine della lettura, quando poi si è palesato in modo chiaro ed evidente la giustezza della loro intuizione di scrivere in comune un libro così impegnativo: *perché proprio ora?* In questa breve introduzione mi auguro di chiarire ai lettori quali sono state le mie risposte e perché mi sento di promuovere la massima diffusione di questo come di altre produzioni letterarie che trattino, purché con analoga competenza, un argomento difficile, ampio ed estremamente serio ed attuale come quello descritto sinteticamente nel titolo di questo libro.

Uno dei più noti browser internazionali sulla propria home page ha posto questo quesito ai suoi utenti: "Nel 2020 ci potrebbero essere circa 30 miliardi di dispositivi connessi a Internet. Che sensazioni ti procura questo scenario?". L'associazione di idee spontanea che mi è sorta leggendo il quesito è stata una frase celebre di uno dei fondatori della Intel, forse la più famosa società produttrice di semiconduttori al mondo che più di tutte ha tratto beneficio dallo sviluppo della tecnologia e di Internet, Andrew Stephen Grove: *Il problema più grande di quest'epoca elettronica riguarda la privacy.* In

effetti sempre più il modo di comunicare, conoscere ed apprendere si sta digitalizzando ed il nostro essere parte della società spesso si configura o meglio si confonde con l'esser connessi, presenti e visibili sui social-network, o comunque sul web. La "visibilità" digitale presenta un confine molto labile tra ciò che vogliamo sia pubblico e ciò che non riusciamo a mantenere "privato". Per fortuna, questo non vale per tutte le persone e non vale in tutte le parti del nostro mondo sempre più globalizzato, ma il trend delle nostre società occidentali appare segnato da un avanzare della tecnologia estremamente più veloce della capacità degli uomini di adeguarsi ai nuovi strumenti ed alle nuove idee e possibilità che queste offrono, soprattutto per quanto riguarda la capacità di cogliere i rischi che queste novità portano con loro.

L'ignoranza verso il tecnologicamente nuovo, intesa come non-conoscenza e cioè ignorare cosa significa o cosa comporta l'uso di una nuova App o di un nuovo Social, espone tutti noi a pericoli o rischi assolutamente inattesi e tantomeno comprensibili nelle loro conseguenze. Di fronte a tutto questo, il singolo utente da solo non può gestire e proteggersi dai rischi che si conoscono e ancor di più da quelli che si sviluppano in modo imprevedibile per l'intera comunità, basti pensare alle conseguenze sulle attività che può avere il cyber-crime o alle conseguenze sociali del cyber-bullismo. Sono le organizzazioni nazionali e sovranazionali che devono farsi carico di prevedere, proteggere ed informare le persone e le attività produttive da quello che il nuovo contesto sociale o tecnologico può determinare o sta già determinando. L'esigenza di regole e di controlli sulle attività private e professionali è dunque una necessità comune assolutamente doverosa da assolvere.

Il nuovo Regolamento Europeo "GDPR" 2016/679 ha raccolto l'esigenza dell'intera comunità europea di tutelarsi in modo omogeneo e condiviso in merito a tutto ciò che riguarda il concetto alla base della privacy, e cioè il diritto alla tutela dei dati e delle informazioni della persona fisica per la salvaguardia della vita privata di ciascun individuo. Questo regolamento definisce ulteriormente, rispetto a quanto già presente, i diritti degli individui e le garanzie affinché questi diritti vengano tutelati da tutti coloro che possono avere a che

fare con le loro informazioni. La tutela dei diritti nasce dal controllo che tutte le possibili entità coinvolte nella gestione delle informazioni personali rispettino le regole previste dal GDPR.

Ed ecco che questo libro, in questo momento, risulta essere uno strumento assolutamente indispensabile per coloro che avranno il compito di provvedere alle verifiche di coerenza ed adeguatezza alla nuova normativa emanata ad aprile 2016. L'obbligo di cogenza è un dovere, ma anche le realtà più volenterose potrebbero incorrere in difficoltà procedurali o tecnologiche che non sono di sicuro di facile soluzione.

La capacità di condurre un audit in ambito privacy completo ed esauriente può essere una competenza sfruttabile dal professionista che si propone sul mercato sia in ambito consulenziale che in ambito di verifica da parte di enti preposti al controllo. In quest'ottica la formazione di competenze sempre più qualificate deve esser vista come un'opera non solo meritoria ma assolutamente necessaria, per acquisire una metodologia chiara e ripetibile dell'attività di verifica, o meglio di audit, delle realtà che devono risultare adeguate alla normativa.

La mia personale esperienza di consulente aziendale, auditor di sistemi di gestione per la sicurezza delle informazioni e responsabile di organismi accreditati per la certificazione di persone e di sistemi di gestione, mi porta a dire che quest'opera sarà di aiuto a due tipologie di lettori:

- il singolo professionista che intende aumentare o migliorare la sua conoscenza in un ambito professionale di sicuro interesse che offrirà moltissime opportunità nell'immediato coinvolgendo tutte le attività produttive, che avranno bisogno di figure professionali capaci e competenti nelle verifiche;
- l'imprenditore o i responsabili della compliance aziendale perché è fondamentale per loro comprendere quanto possa essere impegnativa una sessione di audit in ambito privacy e capire di doversi rivolgere a persone qualificate che abbiano esperienza e metodo per aiutare le loro organizzazioni ad essere conformi a tutto ciò che la normativa richiede.

La piena applicazione del regolamento europeo sulla privacy

(GDPR), è prevista per il 25 maggio 2018, ed entro tale data tutte le realtà che abbiano a che fare con la gestione di dati personali dovranno essere conformi a quanto previsto dal regolamento, pena il rischio di ricevere sanzioni estremamente pesanti, in termini economici e d'immagine. Tale situazione oggettiva non rinviabile porterà al proliferare di richieste di consulenza da parte di tutte quelle realtà che realizzeranno di non esser pronte e conformi alla normativa entro la data sopra citata. Solo coloro i quali avranno provveduto per tempo ad acquisire le giuste competenze potranno proporsi professionalmente sul mercato avendo una visione quanto più ampia e completa di quello che il GDPR richiede.

La privacy ed il rispetto dei requisiti che la nuova normativa prevede spazia in un ambito che investe contemporaneamente aspetti di giurisprudenza, conoscenze tecnologiche approfondite e modalità di verifica che solo degli esperti possono padroneggiare ed è per rispondere a questa esigenza che gli autori hanno deciso di dire la loro sugli argomenti che gli appartengono. Di sicuro un DPO (Data Protection Officer) dovrà avvalersi di esperti nel caso di grandi o specifiche realtà aziendali, ma la sua formazione non potrà prescindere dalla conoscenza di quali devono essere gli argomenti che dovrà supervisionare.

È questo insieme di considerazioni su cosa dice il nuovo regolamento europeo e su quanto di sicuro accadrà nel mercato delle aziende e dei professionisti che offriranno la loro consulenza in ambito privacy, che mi ha portato a rispondere alle domande con le quali ho esordito nella mia prefazione, ed alle quali credo, e spero, di aver risposto con le mie considerazioni.

Questo libro offre tutti gli spunti per confrontarsi con gli autori su quanto il lettore già conosce e quanto, soprattutto, non conosce ed è questo aspetto che mi ha portato a considerare opportuno il mix di competenze degli autori ed il momento particolare della loro pubblicazione.

2. L'attività di audit dal punto di vista giuridico: rapporti con il GDPR (Michele Iaselli)

2.1 Audit e GDPR: introduzione

Come è noto gli enti e le aziende che gestiscono archivi elettronici e dati personali devono fare i conti con il Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). Come prevede l'art. 99, il Regolamento (GDPR) entrerà in vigore il ventesimo giorno successivo alla pubblicazione nella Gazzetta Ufficiale (25 maggio 2016), ma si applicherà a decorrere dal 25 maggio 2018.

Ma perché un Regolamento europeo? La necessità di emanare un Regolamento europeo in materia di protezione dei dati personali nasce dalla continua evoluzione degli stessi concetti di privacy e protezione dei dati personali e quindi della relativa tutela dovuta principalmente alla diffusione del progresso tecnologico.

Originariamente la direttiva 95/46/CE, pietra angolare nell'impianto della vigente normativa dell'UE in materia di protezione dei dati personali, è stata adottata nel 1995 con due obiettivi: salvaguardare il diritto fondamentale alla protezione dei dati e garantire la libera circolazione dei dati personali tra gli Stati membri. Successivamente incalzanti sviluppi tecnologici hanno allontanato le frontiere della protezione dei dati personali. La portata della condivisione e della raccolta di dati è aumentata in modo vertiginoso.

La tecnologia attuale consente alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività e, sempre più spesso, gli stessi privati rendono pubbliche sulla rete mondiale informazioni personali che li riguardano. Le nuove tecnologie non hanno trasformato solo l'economia, ma anche le relazioni sociali. Di conseguenza, pur rimanendo valido in termini di obiettivi e principi, il quadro

giuridico attuale non ha impedito la frammentazione delle modalità di applicazione della protezione dei dati personali nel territorio dell'Unione, né ha eliminato l'incertezza giuridica e la diffusa percezione nel pubblico che le operazioni on line comportino notevoli rischi. È diventato, quindi, necessario instaurare un quadro giuridico più solido e coerente in materia di protezione dei dati nell'Unione che, affiancato da efficaci misure di attuazione, consentirà lo sviluppo dell'economia digitale nel mercato interno, garantirà alle persone fisiche il controllo dei loro dati personali e rafforzerà la certezza giuridica e operativa per i soggetti economici e le autorità pubbliche. Tali aspetti vanno sicuramente presi in considerazione in sede di audit privacy, attività che rappresenta per molte aziende italiane una grande lacuna.

L'Audit Privacy è una valutazione dei processi aziendali sul grado di rispetto della normativa vigente. Si può paragonare a un check up perché va fatto da un esperto indipendente, l'auditor, che potremmo paragonare al medico. In caso di patologie, ovvero di riscontro di qualcosa che va perfezionato in azienda sul fronte della raccolta e trattamento dati, il medico-auditor (che deve essere un esperto di data protection sia a livello giuridico che informatico) prescrive le "cure" del caso. L'audit dal punto di vista pratico consiste in una intervista al titolare del trattamento dati in azienda, che si svolge periodicamente. Le domande sono dirette a conoscere in che modo i dati vengono raccolti e trattati: alle aziende viene chiesto per esempio se esistono già dei sistemi di sicurezza attivi volti a proteggere i dati conservati, dei sistemi di backup, firewall, antispam.

Un aspetto importante relativo ai rapporti tra audit e GDPR è la differenza di traduzione tra la versione italiana e quella inglese dello stesso Regolamento. Nella versione inglese, infatti, il termine audit è citato in 4 articoli (28, 39, 47 e 58), mentre nella versione italiana del Regolamento il termine audit non compare mai. Il termine è infatti stato tradotto con tre diversi termini: revisione, controllo e verifica. Va premesso che per la norma italiana UNI EN ISO 19011:2012 (Linee guida per gli audit dei sistemi di gestione) l'audit è un preciso processo sistematico, indipendente e documentato per ottenere evidenze e valutarle con obiettività, al fine di stabilire in quale misura i

criteri precedentemente individuati sono stati soddisfatti. Tale definizione è ulteriore rispetto al concetto generico di controllo. Un audit richiede che siano rispettate scrupolosamente una serie di regole.

Cosa comporta quindi questa differenza di traduzione? Dal punto di vista della normativa va sottolineato che nessuna traduzione prevale sulle altre e che tutte hanno lo stesso valore giuridico; ma praticamente come si deve comportare l'interprete? E' evidente che la traduzione offerta al lettore italiano non è delle migliori, considerando che nella lingua italiana il termine audit esiste e ha un suo preciso significato. Il testo inglese del GDPR, e lo confermano anche il testo della versione francese (audits) e spagnola (auditorías), richiede, difatti, attività ben più complesse e strutturate di semplici controlli. Prima ancora di evidenziare le regole giuridiche di maggiore rilevanza che costituiscono il punto di riferimento per una completa attività di audit con l'avvento del GDPR, bisogna premettere che alla base della stessa attività di audit è fondamentale una corretta valutazione del rischio che con la diffusione dell'informatica e più nello specifico delle nuove tecnologie ha assunto una rilevanza ancora maggiore.

2.2 Cosa si intende per rischio informatico

A partire dagli anni novanta, con la nascita e conseguente diffusione di Internet, le nuove tecnologie hanno assunto un ruolo sempre più preponderante modificando i rapporti sociali ed individuali, con notevoli ripercussioni in ogni ambito della nostra vita sociale. Con il passar del tempo, Internet è diventato uno strumento di comunicazione di massa, indispensabile nella vita di tutti i giorni, si pensi alle numerose operazioni che compiamo regolarmente utilizzando il Web, quali inviare una candidatura online tramite un form, condividere dei contenuti sui social, acquistare un viaggio o eseguire un'operazione bancaria, ma rappresenta anche un'opportunità inestimabile per lo sviluppo economico delle imprese, come delle istituzioni scientifiche e pubbliche. La rivoluzione digitale sta dunque portando molti benefici a società, imprese, studi professionali ma,