



ORDINE DEI
DOTTORI COMMERCIALISTI E DEGLI
ESPERTI CONTABILI

M I L A N O

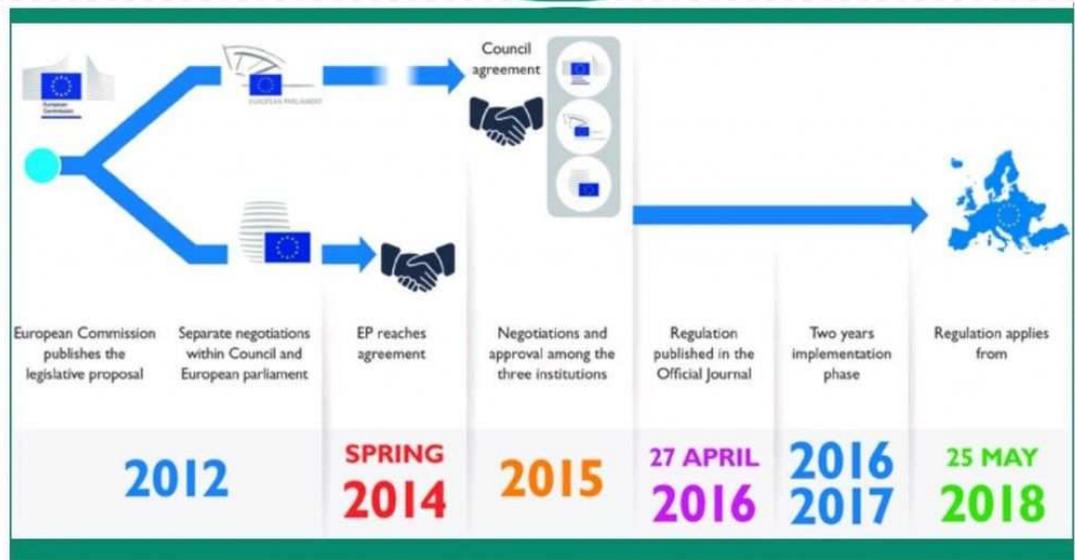


Gdpr e commercialisti

GDPR E COMMERCIALISTI: SFIDE E OPPORTUNITÀ A UN ANNO DALLA PIENA APPLICAZIONE

PATRIZIA GHINI

17 maggio 2019



ORDINE DEI
DOTTORI COMMERCIALISTI E DEGLI
ESPERTI CONTABILI

M I L A N O



CAMBIAMENTO NELLA NORMATIVA DI RIFERIMENTO

Regolamento Generale in materia di protezione dei dati personali 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)

Codice in materia di protezione dei dati personali (Decreto Legislativo n. 196/2003 successive modifiche e integrazioni)

CAMBIAMENTO NELLA FILOSOFIA DELLA NORMATIVA

Codice e RGPD sono informati a due filosofie diverse e che quest'ultimo è basato sulla cd. **accountability** (termine tradotto in italiano con **responsabilizzazione**), in base alla quale il legislatore europeo, in molti casi, rimette la scelta connessa alle caratteristiche principali del trattamento (ivi comprese le misure a protezione degli interessati) al titolare del trattamento che è chiamato

- ad effettuare una valutazione,
- ad assumere una decisione
- a dare prova di avere adottato misure proporzionate ed efficaci

CAMBIAMENTO NEGLI ADEMPIMENTI E NEGLI OBBLIGHI

Sono introdotti vari istituti – quali la valutazione d’impatto privacy, la figura del RPDP, i meccanismi di certificazione –all’insegna di una più accentuata responsabilizzazione di chi opera (anzitutto) in qualità di titolare del trattamento, essendo chiamato a rendere conto delle misure tecnico-organizzative poste in essere per assicurare la liceità dei trattamenti e il rispetto dei diritti fondamentali degli interessati.

- Principi generali del trattamento di dati personali**
- Assicurare la liceità del trattamento di dati personali**
- Trasparenza del trattamento: l'informativa agli interessati**
- Un approccio responsabile al trattamento: Accountability**
- Principio di "responsabilizzazione" dei titolari e responsabili del trattamento: principali elementi**
 - **Rapporti contrattuali fra titolare e responsabile del trattamento**
 - **Registro dei trattamenti**
 - **Misure di sicurezza**
 - **Notifica di una violazione dei dati personali**
 - **Responsabile della protezione dei dati**
- Diritti degli interessati**
- Trasferimento dei dati all'estero**

CAMBIAMENTO NELL'APPROCCIO ALLA NORMATIVA

Il **primo criterio** - sintetizzato dall'espressione inglese "data protection by default and by design" - è quello previsto dall'articolo 25 che impone di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili al fine di

➤ soddisfare i requisiti del Regolamento

➤ tutelare i diritti degli interessati

tenendo conto

➤ del **contesto** complessivo ove il trattamento si colloca

➤ dei **rischi** per i diritti e le libertà degli interessati.

CAMBIAMENTO NELL'APPROCCIO ALLA NORMATIVA

Tutto questo

a) deve avvenire a monte, prima di procedere al trattamento dei dati vero e proprio

➤ sia **al momento di determinare i mezzi del trattamento**

➤ sia **all'atto del trattamento stesso**

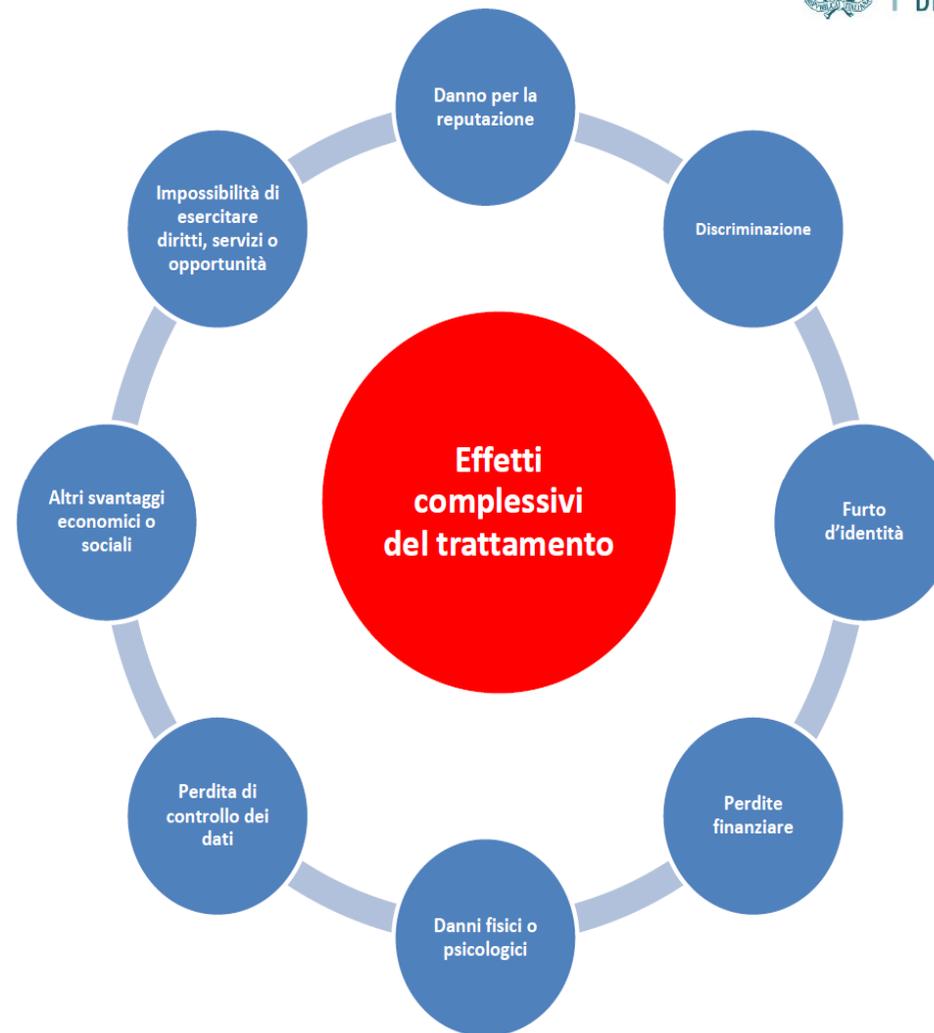
b) richiede, pertanto, un'analisi preventiva e un impegno applicativo da parte dei titolari che devono sostanziarsi in una serie di attività specifiche e dimostrabili.

CAMBIAMENTO NELL'APPROCCIO ALLA NORMATIVA

Il **secondo criterio** individuato nel Regolamento rispetto alla gestione degli obblighi dei titolari è il **rischio inerente al trattamento** da intendersi come rischio di impatti negativi sulle libertà e i diritti degli interessati (considerando 75-77); tali impatti dovranno essere analizzati attraverso un apposito processo di valutazione (artt. 35- 36) tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il titolare ritiene di dover adottare per mitigare tali rischi (si segnalano, al riguardo, le linee-guida in materia di valutazione di impatto sulla protezione dei dati del Gruppo "Articolo 29«.

www.garanteprivacy.it/Regolamentoue/

Tutorial del Garante sul concetto di "rischio"



CAMBIAMENTO NEGLI ELEMENTI DI VALUTAZIONE DEL COMPORTAMENTO DEL TITOLARE

Il Regolamento richiede l'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del Regolamento (**artt. 23-25**, in particolare, e l'intero **Capo IV del Regolamento**).

Viene affidato ai titolari il compito di decidere autonomamente

- le modalità,
- le garanzie e
- i limiti del trattamento dei dati personali,

nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel Regolamento.

CAMBIAMENTO NEL SISTEMA SANZIONATORIO

Al cambio di filosofia fa da contrappeso un più severo quadro sanzionatorio e precisi elementi per la commisurazione delle sanzioni:

- a) la natura, la gravità e la durata della violazione tenendo in considerazione la natura, l'oggetto o a finalità del trattamento in questione nonché il numero di interessati lesi dal danno e il livello del danno da essi subito;
- b) il carattere doloso o colposo della violazione;
- c) le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati;
- d) il grado di responsabilità del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto ai sensi degli articoli 25 e 32;

CAMBIAMENTO NEL SISTEMA SANZIONATORIO

- e) eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento;
- f) il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi;
- g) le categorie di dati personali interessate dalla violazione;
- h) la maniera in cui l'autorità di controllo ha preso conoscenza della violazione, in particolare se e in che misura il titolare del trattamento o il responsabile del trattamento ha notificato la violazione;

CAMBIAMENTO NEL SISTEMA SANZIONATORIO

- i) qualora siano stati precedentemente disposti provvedimenti di cui all'articolo 58, paragrafo 2, nei confronti del titolare del trattamento o del responsabile del trattamento in questione relativamente allo stesso oggetto, il rispetto di tali provvedimenti;
- j) l'adesione ai codici di condotta approvati ai sensi dell'articolo 40 o ai meccanismi di certificazione approvati ai sensi dell'articolo 42; e
- k) eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione.

FOCUS SULLE SCELTE DEL TITOLARE E SUL PROCESSO DECISIONALE

- Governance
- Compliance integrata
- Organizzazione
- Consapevolezza dei rischi
- Competenze

FOCUS SULLA VALUTAZIONE DELLE SCELTE DEL TITOLARE

- Da parte del Dpo (se nominato)
- Da parte degli organi di controllo
- Da parte delle Autorità

FOCUS SUL PROFILO PRIVACY DEL TITOLARE

- Da reattivo a proattivo
- Da formale a sostanziale
- Da statico a dinamico

FOCUS SUI PROCESSI AZIENDALI E SUI PROCESSI DI TRATTAMENTO

- Incorporazione della privacy nei processi di trattamento
- Incorporazione della privacy nei sistemi e negli strumenti di trattamento
- Incorporazione della privacy nelle persone autorizzate al trattamento
- Incorporazione della privacy nei prodotti e nei servizi che si basano sul trattamento di dati personali

Ogni trattamento di dati personali deve avvenire nel rispetto dei principi fissati all'articolo 5 del Regolamento (UE) 2016/679:

- **liceità, correttezza e trasparenza** del trattamento, nei confronti dell'interessato;
- **limitazione** della **finalità** del trattamento, compreso l'obbligo di assicurare che eventuali trattamenti successivi non siano incompatibili con le finalità della raccolta dei dati;
- **minimizzazione** dei dati: ossia, i dati devono essere adeguati pertinenti e limitati a quanto necessario rispetto alle finalità del trattamento;
- **esattezza e aggiornamento** dei dati, compresa la tempestiva cancellazione dei dati che risultino inesatti rispetto alle finalità del trattamento;
- **limitazione** della **conservazione**: ossia, è necessario provvedere alla conservazione dei dati per un tempo non superiore a quello necessario rispetto agli scopi per i quali è stato effettuato il trattamento;
- **integrità e riservatezza**: occorre garantire la sicurezza adeguata dei dati personali oggetto del trattamento.

FOCUS SU PREVENZIONE E GESTIONE VIOLAZIONE DATI PERSONALI

Violazione di sicurezza che comporta accidentalmente o in modo illecito

- la distruzione
- la perdita
- la modifica
- la divulgazione non autorizzata
- l'accesso ai dati personali
- trasmessi, conservati o comunque trattati



ORDINE DEI
DOTTORI COMMERCIALISTI E DEGLI
ESPERTI CONTABILI

M I L A N O



FONDAZIONE
COMMERCIALISTI
ODCEC di MILANO

L'IMPATTO DEL GDPR SULLA PROFESSIONE

Decreto legislativo 28 giugno 2005, n. 139

Art. 1. Oggetto della professione

1 . Agli iscritti nell'Albo dei dottori commercialisti e degli esperti contabili, di seguito denominato "Albo", è riconosciuta competenza specifica in economia aziendale e diritto d'impresa e, comunque, nelle materie economiche, finanziarie, tributarie, societarie ed amministrative.

DECRETO LEGISLATIVO 28 giugno 2005, n. 139

2 . In particolare, formano oggetto della professione le seguenti attività:
a) l'amministrazione e la liquidazione di aziende, di patrimoni e di singoli beni; b) le perizie e le consulenze tecniche; c) le ispezioni e le revisioni amministrative; d) la verifica ed ogni altra indagine in merito alla attendibilità di bilanci, di conti, di scritture e di ogni altro documento contabile delle imprese ed enti pubblici e privati; e) i regolamenti e le liquidazioni di avarie; f) le funzioni di sindaco e di revisore nelle società commerciali, enti non commerciali ed enti pubblici.

CODICE DEONTOLOGICO DELLA PROFESSIONE

Articolo 10 RISERVATEZZA

- 1. Il professionista, fermi restando gli obblighi del segreto professionale e di tutela dei dati personali, previsti dalla legislazione vigente, deve mantenere l'assoluto riserbo e la riservatezza delle informazioni acquisite nell'esercizio della professione e non deve diffondere tali informazioni ad alcuno, salvo che egli abbia il diritto o il dovere di comunicarle in conformità alla legge.*
- 2. Le informazioni acquisite nell'esercizio della professione non possono essere utilizzate per ottenere alcun vantaggio personale del professionista o di terzi.*
- 3. Il professionista vigilerà affinché il dovere di riservatezza sia rispettato anche dai suoi tirocinanti, dipendenti e collaboratori.*

DOCUMENTI CNDC IN MATERIA DI PRIVACY

1. Regolamento in materia di privacy e protezione dei dati personali e informative Norme e Regolamenti

Data di pubblicazione: 25/05/2018

2. 39 - Regolamento (UE) 2016-679 in materia di protezione dei dati personali Note Informative

Data di pubblicazione: 07/05/2018

3. 37 - Il regolamento Ue72016679 General Data Protection Regulation (GDPR) nuove regole comunitarie e precisazioni in materia di protezione dei dati personali. Checklist di base per gli studi Note Informative

Data di pubblicazione: 27/04/2018

DOCUMENTI CNDC IN MATERIA DI PRIVACY

34. Il regolamento Ue/2016/679 General Data Protection Regulation (GDPR): nuove regole comunitarie e precisazioni in materia di protezione dei dati personali Documenti CNDCEC - FNC

Data di pubblicazione: 27/04/2018

25 - Regolamento (UE) 2016-679 in materia di protezione dei dati personali Note Informative

Data di pubblicazione: 27/03/2018

NOTA INFORMATIVA DEL CNDCEC IN MATERIA DI PRIVACY

39 - Regolamento (UE) 2016-679 in materia di protezione dei dati personali

Allegati:

Accordo di contitolarità Fac simile APRI ALLEGATO

Informativa Fornitori Fac Simile APRI ALLEGATO

Informativa Sito Web Fac Simile APRI ALLEGATO

Linee Guida Privacy ORDINI TERRITORIALI APRI ALLEGATO

Nomina DPO Fac Simile APRI ALLEGATO

Nomina responsabile esterno Fac Simile APRI ALLEGATO

Nomina responsabile interno Fac Simile APRI ALLEGATO

PRIVACY E ATTIVITA' DEL COMMERCIALISTA

*..... in via prioritaria occorre dunque distinguere il segmento di attività in cui il consulente del lavoro tratta i dati dei propri dipendenti ovvero dei propri clienti (persone fisiche) nella sua qualità di professionista, attività fiscalmente e normativamente regolamentata, dalla diversa attività (tipica di questo ordine professionale) per la quale il medesimo soggetto tratta i dati dei dipendenti del cliente. Nel **primo caso** il consulente del lavoro agisce in piena autonomia e indipendenza determinando puntualmente le finalità e i mezzi del trattamento dei dati del cliente per il perseguimento di scopi attinenti alla gestione della propria attività. Per tali ragioni, egli ricopre il ruolo di titolare del trattamento (art. 4, par. 1, punto 7, del Regolamento), in quanto non si limita ad effettuare un'attività meramente esecutiva di trattamento, "per conto" del cliente, bensì esercita un potere decisionale del tutto autonomo sulle finalità e i mezzi del trattamento.*

PRIVACY E ATTIVITA' DEL COMMERCIALISTA

*Nel **secondo caso** occorre fare riferimento alla figura del **responsabile**, che, anche in base alla nuova disciplina pienamente in vigore nel nostro ordinamento a far data dal 25 maggio 2018 rimane connotata dallo svolgimento di attività delegate dal titolare il quale, all'esito di proprie scelte organizzative, può individuare un soggetto particolarmente qualificato allo svolgimento delle stesse (in termini di conoscenze specialistiche, di affidabilità, di struttura posta a disposizione, v. considerando 81, Reg. cit.), delimitando l'ambito delle rispettive attribuzioni e fornendo specifiche istruzioni sui trattamenti da effettuare(3). Il titolare pertanto è il soggetto che, alla luce del concreto contesto nel quale avviene il trattamento, assume le decisioni di fondo relative a finalità e modalità di un trattamento lecitamente effettuato in base ad uno dei criteri di legittimazione individuati dall'ordinamento (v. artt. 6 e 9 del Regolamento).*

PRIVACY E ATTIVITA' DEL COMMERCIALISTA

L'articolo 28 del Regolamento (UE) 679/2016 ha semmai, rispetto alla disciplina previgente, precisato e delimitato i compiti che possono essere attribuiti dal titolare al responsabile, individuando espressamente l'ambito delle rispettive responsabilità e gli obblighi di cooperazione cui è tenuto il responsabile esclusivamente in funzione delle attività svolte per conto del titolare (v. artt. 30, 33, par. 2 e 82 del Regolamento).

PRIVACY E ATTIVITA' DEL COMMERCIALISTA

L'articolo 28 del Regolamento (UE) 679/2016 ha semmai, rispetto alla disciplina previgente, precisato e delimitato i compiti che possono essere attribuiti dal titolare al responsabile, individuando espressamente l'ambito delle rispettive responsabilità e gli obblighi di cooperazione cui è tenuto il responsabile esclusivamente in funzione delle attività svolte per conto del titolare (v. artt. 30, 33, par. 2 e 82 del Regolamento).

*In definitiva, secondo il costante orientamento espresso dall'Autorità, le **attività di trattamento svolte da soggetti esterni per conto del titolare**, il quale può decidere di affidare all'esterno lo svolgimento di compiti strettamente connessi all'esecuzione di obblighi previsti dalla normativa lavoristica e/o dal contratto di lavoro, devono, di regola, essere inquadrare nello **schema titolare/responsabile del trattamento**.*

PRIVACY E ATTIVITA' DEL COMMERCIALISTA

L'Autorità, vigente la precedente disciplina, si è espressa sulla qualificazione in termini di titolare o responsabile di alcune figure che effettuano trattamenti di dati personali, anche nell'ambito del rapporto di lavoro, all'esito dell'esame - effettuato sul piano sostanziale e non formale - delle attività in concreto svolte. Più specificamente, a titolo esemplificativo, il Garante ha ritenuto che rivesta, di regola, il ruolo di responsabile la società capogruppo delegata da società controllate e collegate a svolgere adempimenti in materia di lavoro, previdenza ed assistenza sociale per i lavoratori, il soggetto che fornisce servizi di localizzazione geografica, i servizi di posta elettronica, i servizi di televigilanza.

PRIVACY E FATTURAZIONE ELETTRONICA

Gli intermediari e gli altri soggetti delegati assumono, in tale contesto, il ruolo di responsabile o sub-responsabili del trattamento, a seconda delle scelte organizzative degli operatori economici e dei relativi modelli contrattuali utilizzati.

Il Garante ha formulato alcuni rilievi critici in relazione ad alcuni modelli contrattuali utilizzati dalle maggiori società produttrici di software gestionale e fiscale, che evidenziano elevati rischi di utilizzi impropri dei dati personali nell'ambito dei trattamenti effettuati dagli intermediari e dagli altri soggetti delegati dagli operatori economici nel processo di fatturazione

PRIVACY E FATTURAZIONE ELETTRONICA

Sono state rilevate altresì peculiari modalità di articolazione dei ruoli assunti nel trattamento dei dati personali oggetto della fatturazione elettronica, che non ripartiscono correttamente le responsabilità circa i rischi derivanti dal trattamento, introducendo sproporzionati esoneri di responsabilità, soprattutto in caso di contratti standard, con margini di negoziazione pressoché nulli in capo al titolare del trattamento.

ATTIVITA' DI VIGILANZA COLLEGIO SINDACALE

*La vigilanza, nel suo effettivo svolgimento deve seguire, quale efficiente modalità operativa, un **sistema di selezione impostato su un risk approach**, ossia basato sull'identificazione e la valutazione del rischio che il mancato rispetto della normativa e dei principi di corretta amministrazione possa comportare.*

*Il collegio sindacale si avvale, per lo svolgimento dei propri compiti, di **strutturati flussi informativi provenienti dall'organo amministrativo, dal Comitato Controllo e Rischi ove presente e dalle funzioni e dai ruoli di controllo.** Quelli provenienti dalle funzioni operative e/o di controllo della società possono essere oggetto di procedure aziendali che li regolamentano al fine di efficientare il processo.*

ATTIVITA' DI VIGILANZA COLLEGIO SINDACALE

*All'inizio dell'incarico, e poi periodicamente, il collegio verifica, sulla base dei flussi informativi acquisiti, che **la struttura organizzativa e le procedure interne siano idonee a garantire che la società operi in conformità alla normativa legislativa e regolamentare, alle disposizioni dello statuto e, nelle società che abbiano dichiarato di attenersi a codici di comportamento, alle regole di governo societario previste da detti codici.***

L'attività di vigilanza nel suo concreto svolgimento deve quindi intendersi circostritta alle norme che concretamente, con riferimento alla struttura e alle attività della società, possano essere ritenute critiche in ragione della rilevanza del rischio che il loro mancato rispetto possa comportare per la società.

ATTIVITA' DI VIGILANZA COLLEGIO SINDACALE

*Il collegio sindacale vigila sull'**adeguatezza dell'assetto organizzativo** della società.*

Per assetto organizzativo si intende il complesso delle direttive e delle procedure stabilite per garantire che il potere decisionale sia assegnato ed effettivamente esercitato a un appropriato livello di competenza e responsabilità.

ATTIVITA' DI VIGILANZA COLLEGIO SINDACALE

collegio sindacale vigila sull'adeguatezza e sull'efficacia del sistema di controllo interno e gestione dei rischi tenendo conto delle dimensioni e della complessità della società.

Il sistema di controllo interno può essere definito come l'insieme delle direttive, delle procedure e delle prassi operative adottate dall'impresa allo scopo di raggiungere, attraverso un adeguato processo di identificazione, misurazione, gestione e monitoraggio dei principali rischi, i seguenti obiettivi:

..... obiettivi di conformità, volti a assicurare la conformità delle attività aziendali, alle leggi e ai regolamenti in vigore.

ATTIVITA' DI VIGILANZA COLLEGIO SINDACALE

GUIDA OPERATIVA

ATTIVITÀ DI VIGILANZA DEL COLLEGIO SINDACALE DELLE SOCIETÀ NON QUOTATE NELL'AMBITO DEI CONTROLLI SULL'ASSETTO ORGANIZZATIVO

1. CARATTERI GENERALI DELL' "ASSETTO ORGANIZZATIVO
2. ADEGUATEZZA DELL'ASSETTO ORGANIZZATIVO
3. ATTIVITÀ DI VERIFICA DI UN ASSETTO ORGANIZZATIVO
 - 3.1 Chiara identificazione delle funzioni, dei compiti e delle linee di responsabilità
 - 3.2 Esercizio dell'attività decisionale e direttiva della Società da parte dei soggetti ai quali sono attribuiti i relativi poteri
 - 3.4 Presenza di direttive e di procedure aziendali, loro aggiornamento ed effettiva diffusione
 - 3.5 Adeguatezza del sistema di Information Technology



ORDINE DEI
DOTTORI COMMERCIALISTI E DEGLI
ESPERTI CONTABILI

M I L A N O



FONDAZIONE
COMMERCIALISTI
ODCEC di MILANO

COME GARANTIRE E DIMOSTRARE LA CONFORMITÀ

Titolo

- Mettere in atto misure adeguate ed efficaci ed essere in grado di dimostrare la conformità delle attività di trattamento con il regolamento, compresa l'efficacia delle misure
- Mettere in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati
- Facilitare l'applicazione efficace della legislazione sulla protezione dei dati personali

Titolo

- ❑ *La UNI/PdR 43.2.2018 è applicabile a tutte le organizzazioni che, in qualità di titolari e/o responsabili del trattamento, gestiscono dati personali con strumenti ICT ed è finalizzata a fornire un insieme di requisiti che permetta a questi soggetti, di essere conformi a quanto previsto dal quadro normativo europeo e nazionale in modo efficace.*
- ❑ *Questo schema dovrebbe essere integrato con gli altri processi del titolare ed in particolare con quelli che trattano dati personali anche al fine di assicurare che la protezione dei dati personali sia considerata by design e by default.*

Titolo

- ❑ *Il titolare dovrebbe assicurare che vi siano responsabilità, autorità e competenza appropriate per trattare i dati personali in genere con specifico riferimento all'attuazione e mantenimento del processo di gestione dei dati personali e l'assicurazione della sua adeguatezza, efficacia ed efficienza di tutti i controlli.*
- ❑ *Le misure di sicurezza da adottare devono essere di natura organizzativa, di processo, e tecnologiche, devono essere formalizzate e devono essere rese efficaci tramite l'adozione di idonei strumenti che ne permettano la adeguata applicazione.*

Titolo

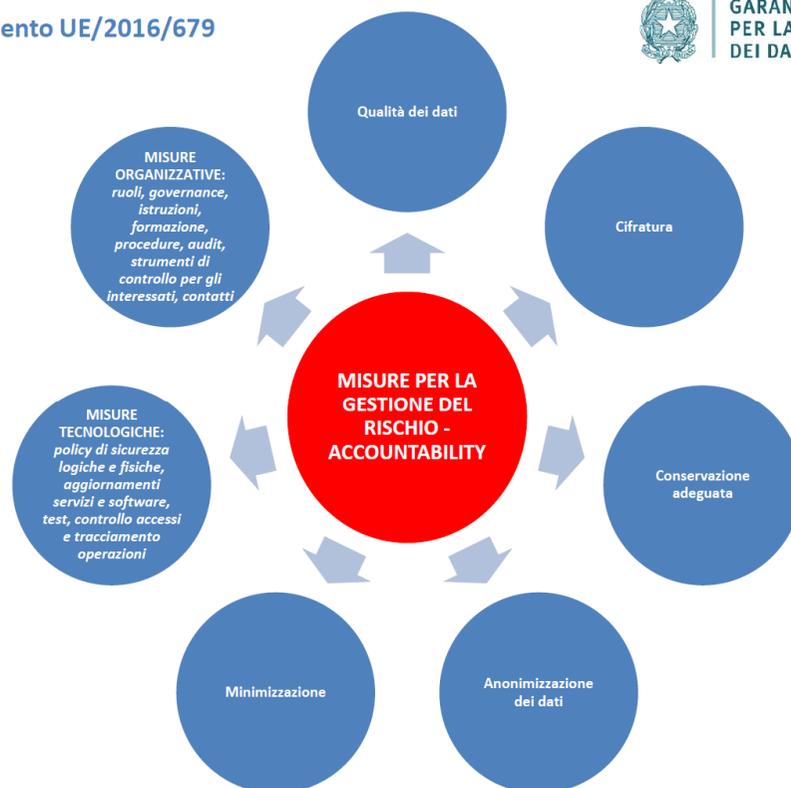
- ❑ *Per questa ragione è indispensabile che siano state svolte le necessarie verifiche su ognuno di questi domini, al fine di determinare come l'organizzazione intende proteggere i dati personali che tratta, con quali strumenti e che l'attuazione sia sufficientemente efficace.*
- ❑ *Valutazione sulla continua idoneità, adeguatezza ed efficacia e efficienza.*
- ❑ *Con la ponderazione dei rischi si perviene alla conclusione della fase di "Valutazione dei rischi" producendo risultati tesi a massimizzare l'efficacia, e l'efficienza delle misure di trattamento dei rischi assunti. Ma si perviene, soprattutto, ad effettuare misurazioni nel continuo dei rischi, al fine di verificare l'emergere di rischi prima ritenuti poco significativi per l'organizzazione.*
- ❑

Focus su SCELTE IN TERMINI DI MISURE TECNICHE E MISURE ORGANIZZATIVE

Regolamento UE/2016/679



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI



ORDINE DEI
DOTTORI COMMERCIALISTI E DEGLI
ESPERTI CONTABILI

M I L A N O

Fonte Studio Patrizia Ghini Milano - Tutti i diritti riservati



Misure organizzative

Secondo standard ISO si intendono

- Politiche
- Procedure
- Regolamenti

idonei ad ottenere un livello di sicurezza e protezione delle informazioni (dei dati) coerente con gli obiettivi e le strategie dell'organizzazione.

Misure organizzative

Sono misure organizzative quelle che:

- prevedono la separazione dei compiti;
 - contemplano ed individuano ruoli e responsabilità;
 - permettono la gestione degli utenti, dei loro diritti, degli accessi fisici;
- consentono la rintracciabilità, la misurazione, i controlli e le verifiche;
- promuovono l'istruzione e la promozione della consapevolezza.

Misure organizzative

- Sensibilizzazione e formazione del personale
- Registrazione delle operazioni (tracciabilità) e delle operazioni di trattamento
- Procedure e istruzioni a responsabili e incaricati

L'arma per tutelare i dati è uno staff ben preparato

Pagina accanto di
Valeria Uva

Il punto debole della tecnologia? Le persone. Anche negli studi professionali le strategie di difesa dagli attacchi informatici e dai furti di dati si basano - oltre che sulle protezioni tecnologiche - soprattutto sulla formazione del personale. Ed è proprio il training il capitolo più corposo delle linee guida per la cybersecurity negli studi legali elaborate dall'Iba (International bar association), l'associazione che riunisce i legali di tutto il mondo.

L'obiettivo di partenza è quello di tutelare le realtà professionali medio-piccole, compresi i singoli professionisti, che non hanno né la disponibilità economica né la preparazione tecnica per dotarsi di strumenti potenti in grado di fronteggiare gli attacchi degli hacker. «Gli studi più piccoli tendono a considerarsi bersagli minori di questi attacchi - si legge nel documento - ma al contrario gli hacker hanno proprio loro nel mirino perché sanno che le loro difese sono più facili da aggirare».

Anche per questo motivo le linee guida Iba suggeriscono agli studi legali (ma di fatto il consiglio si adatta a qualsiasi altra professione) di investire piuttosto nella formazione del personale, che ha costi più contenuti e risultati duraturi nel tempo.

Diffuse già in versione cartacea durante il congresso Iba a Roma in ottobre, ora le linee guida sono disponibili sul sito in versione "personalizzabile", incrociando i dati relativi alla dimensione dello studio e

alla tipologia di intervento si può cioè ottenere uno schema su misura con i suggerimenti di azioni da intraprendere, sempre graduate a seconda della grandezza dimensionale. Ovviamente quello che per una piccola realtà è solo auspicabile, per una media struttura (che nel modello Iba equivale a uno studio con più di 40 persone) può diventare obbligatorio (si veda una sintesi degli interventi nella scheda rielaborata qui a fianco).

L'enfasi sulla formazione

Secondo le linee guida il training del personale deve partire dall'uso corretto delle password, comprese quelle personali. Al di là delle raccomandazioni più ovvie sulla necessità di non trascriverle su fogli accessibili, o di evitare l'uso di nomi e dati personali per costruirle, il documento fornisce anche suggerimenti meno consueti. Al personale viene raccomandato intransigentemente di distinguere le password private da quelle di lavoro evitando il riuso su più siti. Se poi si deve accedere a un sito in modo solo occasionale meglio inventare una sequenza casuale di caratteri e puntare in caso di un secondo accesso sul reset, piuttosto che sulla memorizzazione.

Da tenere sotto controllo anche tutto ciò che viene postato dai professionisti o dai dipendenti sui social media. Non tutti realizzano, ad esempio, che persino le foto dell'ufficio possono fornire agli hacker (e non solo) una miniera di informazioni sulla dislocazione fisica degli spazi. Anche per quanto riguarda

Da valutare la stipula di una polizza assicurativa che può coprire anche i danni da violazione privacy

l'arrivo di mail sospette, il personale andrebbe istruito in dettaglio. Non solo con l'invito a non aprire allegati o cliccare su link pericolosi: lo studio potrebbe fare un passo avanti se chiedesse allo staff di non cancellare la mail ma di segnalargli magari creando un indirizzo dedicato. Questo permetterebbe agli esperti di analizzare meglio i rischi ma anche - si legge nelle note - «di capire come hanno fatto certe mail sospette a superare le barriere di sicurezza». Per verificare il grado di preparazione del personale si potrebbe anche simulare un test con una finta mail di phishing o sospetta. A costi contenuti.

Le altre azioni

Decisamente abordabili anche per i piccoli studi le azioni di miglioramento delle password e di introduzione di autenticazioni multivelo (considerate indispensabili sulle applicazioni più comuni quali Gmail, Yahoo, LinkedIn etc.). La creazione di una policy aziendale per la cybersecurity è un processo che secondo l'Iba dovrebbe essere risparmiato solo al professionista singolo, mentre a tutti si consiglia di proteggersi attraverso una polizza assicurativa che può aiutare a coprire le spese oltre che della perdita dei dati anche legate alla violazione della privacy, al contenzioso e alla diminuzione degli incassi. Così come tutti sono invitati a identificare quali dati sensibili sono trattati dallo studio e a quale livello di protezione. Ma in questo caso il consiglio è di rivolgersi a un professionista su bianco nelle agende.

LEGENDA:

- FACOLTATIVO
- CONSIGLIATO
- RICHIESTO
- OBBLIGATORIO

Precauzioni graduate

Misure di sicurezza contro gli attacchi informatici indicate dalle linee guida Iba e modulate in base alla grandezza dello studio

TIPOLOGIA	PROFESSIONISTA SINGOLO	PICCOLO STUDIO (FINO A 20 PERSONE)	MEDIO STUDIO (DA 21 A 40 PERSONE)
DOTAZIONE TECNOLOGICA			
Utilizzo connessioni internet sicure	●	●	●
Implemento conservazione e sistemi di recupero dati	●	●	●
Criptare dati e strumenti	●	●	●
Segmentare la rete	●	●	●
Utilizzo dispositivi mobili sicuri	●	●	●
PROCESSI ORGANIZZATIVI			
Implemento di username e password sicure abbinata ad autenticazione multipla	●	●	●
Identificazione di dati sensibili e implementazione di protocolli di protezione	●	●	●
Creazione di una policy per la cybersecurity in linea con i rischi individuati	●	●	●
Sviluppo di piani per la continuità aziendale in caso di attacco	●	●	●
Miglioramento del controllo rischi su fornitori e parti terze	●	●	●
Polizza di responsabilità per la cybersecurity	●	●	●
CONTROLLI DI SICUREZZA			
Elenco dei dispositivi ammessi e vietati	●	●	●
Verifiche periodiche sulla vulnerabilità e sulla protezione	●	●	●
Antivirus	●	●	●
Controlli degli accessi da remoto	●	●	●
Software di sicurezza per le app	●	●	●
LINEE DI CONDOTTA			
Indicazioni sui pericoli nell'uso dei social media	●	●	●
Segnalazione di qualsiasi attività sospetta sul computer (improvvisa apertura di finestre, mouse che si muove in maniera indipendente, mail non richieste)	●	●	●
No all'apertura di allegati o link in mail non richieste	●	●	●
Periodici incontri formativi sul phishing	●	●	●
Policy aziendali con protocolli sull'uso di sistemi mail e cloud (mail, Dropbox, OneDrive, Google, Yahoo, etc.)	●	●	●

Fonte: Studio Patrizia Ghini Milano. Tutti i diritti riservati



La CNIL lance sa formation en ligne sur le RGPD ouverte à tous

11 mars 2019

Une nouvelle formation en ligne ouverte à tous (MOOC) intitulée « L'atelier RGPD » propose aux professionnels de découvrir ou mieux appréhender le RGPD. Il permet ainsi d'initier une mise en conformité de leur organisme et d'aider à la sensibilisation des opérationnels.



100%



ORDINE DEI
DOTTORI COMMERCIALISTI E DEGLI
ESPERTI CONTABILI

M I L A N O

Fonte Studio Patrizia Ghini Milano - Tutti i diritti riservati





Grazie per l'attenzione!
Volentieri a disposizione!
Patrizia Ghini

Cell. 345/6573995
e-mail
patriziaghini@patriziaghini.it