30° L'IMPRESA DELLA CONOSCENZA CONTINUA 1988 • 2018

NOTIZIE

n. 026 - SETTEMBRE 2018

LA CONOSCENZA GENERA LE IDEE PER L'INNOVAZIONE DELLE IMPRESE

Aggiornamenti legislativi, normativi, tecnologici e organizzativi per migliorare il sistema di gestione aziendale

PUBBLICATO IL D.LGS. 101/2018 CHE DETTA LE DISPOSIZIONI PER L'ADEGUAMENTO DELLA NORMATIVA NAZIONALE ALLE DISPOSIZIONI DEL REG. (UE) n. 679/2016 [GDPR]

PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI NONCHÉ ALLA LIBERA CIRCOLAZIONI DI TALI DATI

Dott. Ing. L. DI COSMO
- Project Manager Gruppo 2G Management Consulting
- Consulente della normativa sulla protezione dei dati (PRIVACY OFFICER)
- Consulente di Sistemi di Gestione Qualità, Ambiente e Sicurezza;
- Esperto di norme sulla Salute e Sicurezza nei luoghi di Lavoro (D.Lgs. 81/08 s.m.i.)

Dott. Ing. A. SALISBURGO
- Project Manager del Gruppo 2G Management Consulting
- Consulente di Sistemi di Gestione per la Qualità, Ambiente e Sicurezza
- Consulente di Modelli di Organizzazione, Gestione e Controllo (D.Lgs. 231/01 s.m.i.)
- Internal Audit in outsourcing
- Esperto di Sistema di Gestione della Privacy

Dott. Ing. I. CECCARINI
- Consulente di Sistemi di Gestione per la Qualità, Ambiente, Sicurezza e per la Responsabilità Sociale d'Impresa.
- Docente di Corsi per la Sicurezza
- Consulente per la redazione della comunicazione di informazioni di carattere non finanziario
- Consulente per la redazione del Sistema di Gestione dei Dati Personali REG.(UE) n. 679/2016

Dott. Ing. M. BROVERO
- Consulente di Sistemi di Gestione per la Qualità, Ambiente, Sicurezza e per la Responsabilità Sociale d'Impresa.
- Docente di Corsi per la Sicurezza
- Consulente per la redazione del Sistema di Gestione dei Dati Personali REG.(UE) n. 679/2016

1. INTRODUZIONE

È stato pubblicato sulla Gazzetta Ufficiale del 04.09.2018 il decreto legislativo (D.Lgs. 101/2018) che coordina la "vecchia" norma giuridica (D.Lgs. 196/2003), relativa al "Codice in materia di protezione dei dati personali", con il nuovo Regolamento Europeo [Reg. (UE) n. 679/2016] relativo alla *"...protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati..."*.

Il D.Lgs. 101/2018 entrerà in vigore il 19.09.2018.

Il decreto, dall'art. 1 all'art. 16, apporta le modifiche al D.Lgs. 196/2003 con la sostituzione e/o l'aggiunta di parole, articoli e/o riferimenti al Regolamento. L'art. 17 apporta le modifiche al D.Lgs. 150/2011 ("Disposizioni complementari al codice di procedura civile in materia di riduzione e semplificazione dei procedimenti civili di cognizione...").
Il CAPO VI del D.Lgs. 101/2018 (dall'art. 18 all'art. 27) riporta le disposizioni transitori, finali e finanziarie.

Il decreto specifica quali parti del codice in materia di protezione dei dati personali (D.Lgs. 196/2003) sono salvate poiché compatibili con il nuovo assetto definito dal GDPR (General Data Protection Regulation) e cioè dal Reg. (UE) n. 679/2016.

Il decreto si occupa anche delle sanzioni penali poiché vengono recuperate alcune fattispecie penali come il trattamento illecito dei dati personali, l'acquisizione fraudolenta, le false dichiarazioni rese al Garante.

UNA IMPRESA DELLA CONOSCENZA E DI SERVIZI INNOVATIVI

GRUPPO 2G MANAGEMENT CONSULTING

Gruppo 2G Management Consulting s.r.l.
Largo Re Umberto, 106 • 10128 - Torino Tel. 011. 50.50.62 (r.a.) • Fax 011. 50.46.60
www.gruppo2g.com e-mail: gruppo2g@gruppo2g.com

Per quanto riguarda i poteri di indirizzo e semplificazione per micro, piccole e medie imprese, il decreto, dopo l'art. 154 del Regolamento UE inserisce l'art. 154-bis (poteri) in cui si esplicita che il Garante ha il potere di:

"…4. In considerazione delle esigenze di semplificazione delle micro, piccole e medie imprese, come definite dalla Raccomandazione 2003/361/CE, il Garante per la protezione dei dati personali, nel rispetto delle disposizione del Regolamento e del presente Codice, promuove, nelle linee guida adottate a norma del comma 1, lettera a), modalità semplificate di adempimento degli obblighi del titolare del trattamento...".

2. REG. (UE) n. 679/2016 (GDPR)

Il Regolamento (UE) n. 679/2016 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)"*, per le imprese non si configura come una normale nuova legge ma come una innovazione organizzativa e gestionale che deve collocarsi all'interno di uno scenario giuridico nuovo in cui l'organizzazione è sempre più soggetto responsabile (si pensi alla responsabilità amministrativa ex D.Lgs. 231/2001, e alla responsabilità nell'ambito della certezza del diritto nei rapporti tra fisco e contribuente ex D.Lgs. 128/2015).

La conformità delle attività aziendali alle disposizioni normative si attua sia attraverso il rispetto delle disposizioni di legge sia attraverso impegni presi con i vari portatori di interesse e definiti da policy, codici etici o comportamentali stabiliti direttamente dall'organizzazione.

Il Regolamento (UE) 679/2016 non può quindi non prescindere da un "modello di organizzazione e controllo" che vede la protezione dei dati personali come elemento ricorrente nei vari processi aziendali e che riguarda i diritti garantiti all'interessato, la sicurezza dei dati, le procedure di gestione/controllo nonché la contrattualistica.

Il nuovo Regolamento Europeo sulla Privacy (GENERAL DATA PROTECTION REGULATION – GDPR) è entrato in vigore il 24.05.2016 e le norme sono applicabili dal 25 maggio 2018. Con la pubblicazione del decreto di armonizzazione (D.Lgs. 101/2018) di tale Regolamento, si chiude il ciclo delle norme giuridiche applicabili ai dati personali.

Il legislatore europeo ha introdotto una serie di innovazioni non solo per il singolo cittadino ma anche per aziende, enti pubblici, liberi professionisti ed associazioni. Per questo il Reg. (UE) definisce regole più chiare in merito all'informativa ed al consenso dei dati personali stabilendo precisi limiti al loro trattamento automatizzato nonché alla relativa violazione ed all'interscambio degli stessi al di fuori della Comunità Europea.

La definizione di dato personale è riportata nell'articolo 4 del Reg. (UE) n. 679/2016: «DATO PERSONALE»: *qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*.

Lo sviluppo della tecnologia come ad esempio la proliferazione di IoT (Internet of Things) incrementa la raccolta di dati personali. Infatti l'IoT è una infrastruttura costituita dell'interconnessione di servizi di oggetti di uso quotidiano (sensori di rilevamento, posizionati sul campo [es. smartwatch], …) che raccoglie dati personali, li elabora e li trasferisce in rete interagendo con altri dispositivi e oggetti.

Trattamento e profilazione sono quindi due attività che sono state opportunamente definite nel Reg. (UE).

- TRATTAMENTO: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.
- PROFILAZIONE: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute e le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica.

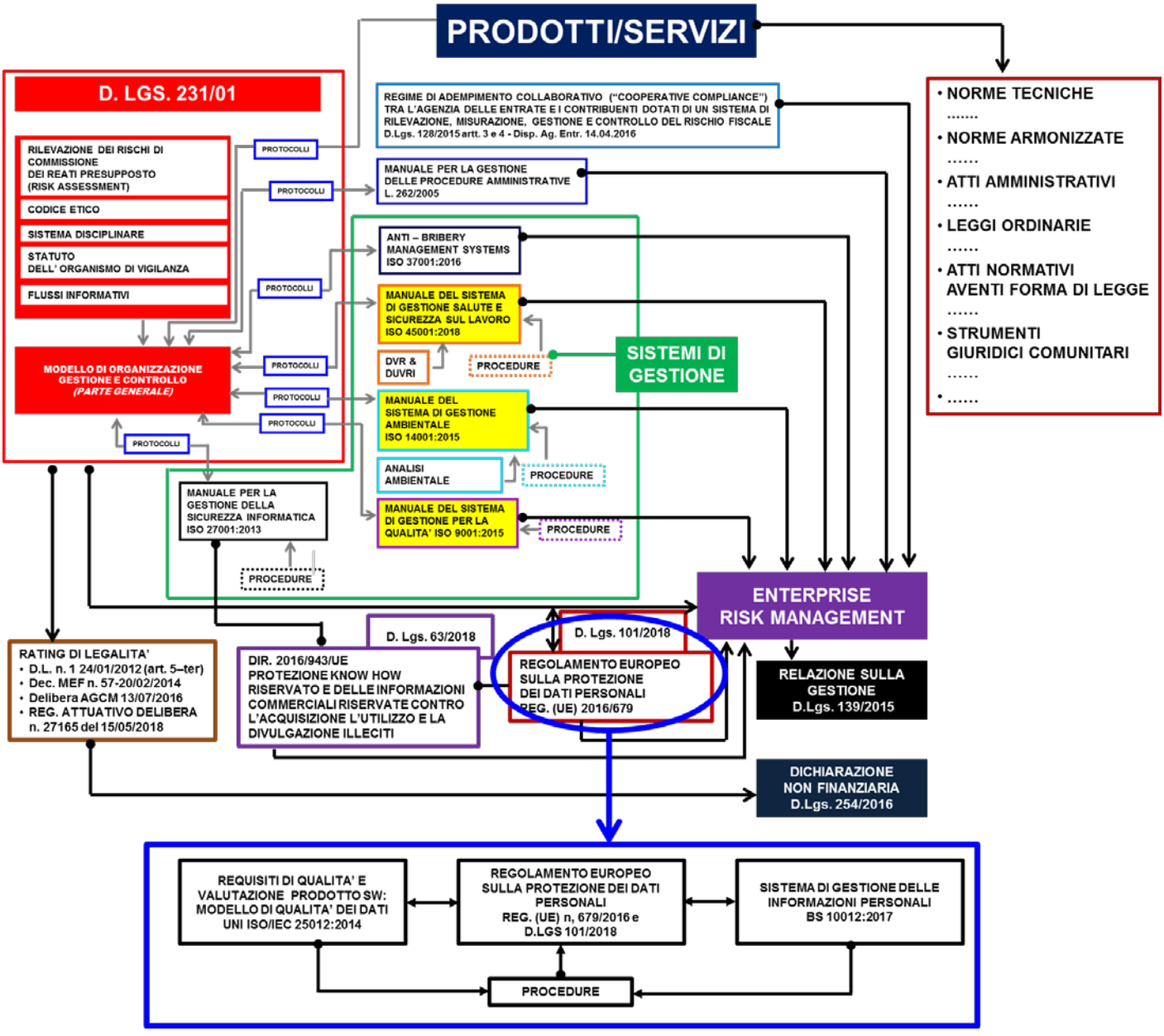
La violazione dei dati personali (Data Breach) richiederà maggiore informazione verso l'interessato e una comunicazione tempestiva ed obbligatoria verso l'autorità nazionale per la protezione dati. Per le aziende cambia radicalmente la visione generale che passa da un censimento dei trattamenti effettuati relativi alla privacy ad un vero e proprio Sistema Rischi dove si riportano gli elementi della privacy ad elementi di rischio per il quale si devono fare misurazioni, mettere in atto politiche di riduzione del rischio e pianificare i costi che vanno ad impattare sul conto economico dell'impresa.

GRUPPO 2G MANAGEMENT CONSULTING

Gruppo 2G Management Consulting s.r.l.
Largo Re Umberto, 106 • 10128 - Torino Tel. 011. 50.50.62 (r.a.) • Fax 011. 50.46.60
www.gruppo2g.com e-mail: gruppo2g@gruppo2g.com

I legislatori europei hanno voluto dichiarare in modo evidente l'importanza del provvedimento stabilendo forti sanzioni pecuniarie nel caso di non rispetto della norma (art. 83, Reg. (UE) n. 679/2016 "Sanzioni"). Una ulteriore novità è rappresentata dall'inserimento del Sistema di Gestione dei Dati Personali nel contesto di una visione sistemica che coinvolge anche la Responsabilità Amministrativa dell'Azienda per i reati presupposto di cui all'art. 24-bis D.Lgs. 231/01 (Delitti Informatici e trattamento illecito di dati).

La gestione dei dati personali deve quindi essere integrata nel Sistema di Gestione Aziendale con i vantaggi di una maggiore e più concreta attenzione alla privacy, con una riduzione dei rischi, con una maggiore chiarezza complessiva e con una riduzione dei costi di trattamento. Si tratta cioè di operare con una visione olistica che superi l'approccio meramente informatico e che integri i "sistemi di gestione" in un processo armonico così come illustrato nello schema sottostante.



GRUPPO 2G MANAGEMENT CONSULTING
Gruppo 2G Management Consulting s.r.l.
Largo Re Umberto, 106 • 10128 - Torino Tel. 011. 50.50.62 (r.a.) • Fax 011. 50.46.60
www.gruppo2g.com e-mail: gruppo2g@gruppo2g.com

30° L'IMPRESA DELLA CONOSCENZA CONTINUA 1988 • 2018

NOTIZIE

n. 026 - SETTEMBRE 2018

LA CONOSCENZA GENERA LE IDEE PER L'INNOVAZIONE DELLE IMPRESE

Aggiornamenti legislativi, normativi, tecnologici e organizzativi per migliorare il sistema di gestione aziendale

3. NOVITÀ VS IL D.LGS. 196/03

Rispetto alle prescrizioni del D.Lgs. 196/03 "Codice in materia di protezione dei dati personali", il Reg. (UE) ha introdotto una serie di novità che devono essere valutate nell'ambito di ogni singola realtà aziendale. Sono stati introdotti nuovi diritti per la persona: come ottenere un intervento umano, esprimere opinioni e contestare il processo automatizzato (art. 22 Reg. (UE) n. 679/2016), la portabilità dei dati (art. 20), nonché la privacy by design e by default (art. 25).

Cambiano le modalità di gestione delle informazioni all'interessato qualora i dati personali non siano o siano raccolti presso l'interessato (art. 13 e art. 14); cambiano le condizioni per il consenso (art. 7 e art. 8); cambia la modalità di trasferimenti di dati personali verso terzi (art. 44-50); cambia il diritto al risarcimento per una violazione al Reg. (UE) e si individua la responsabilità nel titolare e/o responsabile del trattamento (art. 82).

Il Reg. (UE) introduce novità nell'ambito di nuove comunicazioni come la notifica in caso di rettifica, cancellazione o limitazione (art. 19), la notifica di una violazione dei dati personali all'autorità di controllo (art. 33) nonché la comunicazione di una violazione dei dati personali all'interessato (art. 34).

Per quanto riguarda nuove incombenze organizzative il Reg. (UE) introduce i registri delle attività di trattamento (art. 30), la valutazione d'impatto sulla protezione dei dati (art. 35), la consultazione preventiva dell'autorità di controllo (art. 36) quando il trattamento presenta un rischio elevato, la designazione del responsabile della protezione dei dati (art. 37) quando necessario, il contratto o altro atto giuridico con il responsabile del trattamento da parte del titolare del trattamento (art. 28), il diritto alla cancellazione (art. 17), la certificazione della protezione dei dati a dimostrazione della conformità al Reg. (UE) n. 679/2016 (art. 42).

Già nel "considerando" 160 del Reg (UE) viene richiamata la necessità per cui *"…dovrebbe essere incoraggiata l'istituzione di meccanismi di certificazione e sigilli nonché marchi di protezione dei dati che consentano agli interessati di valutare rapidamente il livello di protezione dei dati dei relativi prodotti e servizi…"*.
Inoltre l'aspetto "certificativo" viene richiamato agli artt. 24, 25, 28 e 32 del Reg. (UE). In particolare l'art. 25 al paragrafo 3 così recita: *"…un meccanismo di certificazione approvato ai sensi dell'art. 42 può essere utilizzato come elemento per dimostrare la conformità ai requisiti di cui ai paragrafi 1* [attuare in modo efficace i principi di protezione dei dati] *e 2* [trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento] *del presente articolo…"*.

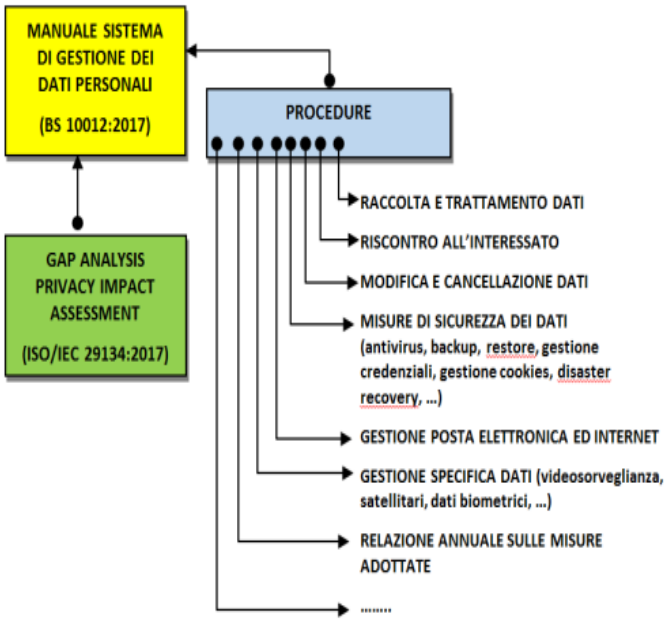
La certificazione della protezione dei dati non riduce la responsabilità del titolare del trattamento o del responsabile del trattamento rispetto alla conformità al Reg. (UE) ma attenua le sanzioni amministrative pecuniarie. Infatti l'art. 83 del Reg. (UE) n. 679/2016 al co.2 lett. J) così recita: *"… al momento di decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa in ogni caso si tiene debito conto dei seguenti elementi: […] j) l'adozione ai […] meccanismi di certificazione approvati ai sensi dell'art. 43 …"*.

4. DESCRIZIONE DEL PROGETTO CONSULENZIALE

Il progetto consulenziale, ideato e sviluppato dal Gruppo 2G Management Consulting, in conformità al Reg. (UE) n. 679/2016 e al D.Lgs. 101/2018 prevede le seguenti fasi:

- Check up aziendale: valutazione dettagliata della situazione esistente (descrizione dei flussi di informazioni), anche in riferimento alle soluzioni operative per l'adeguamento al Reg. (UE) previste a seguito dell'attività preliminare di GAP ANALYSIS.
- Adeguamento al Reg. (UE) dal punto di vista normativo con idonea documentazione: predisposizione e gestione della documentazione a supporto della conformità legislativa.

La documentazione è individuata nello schema sottostante.



Qui sono indicate solamente alcune procedure; altre procedure potranno essere redatte come ulteriore singolo documento o integrate nei capitoli del Manuale del Sistema di Gestione dei Dati Personali in funzione della specificità e complessità organizzativa dell'azienda.

GRUPPO 2G MANAGEMENT CONSULTING

Gruppo 2G Management Consulting s.r.l.
Largo Re Umberto, 106 • 10128 - Torino Tel. 011. 50.50.62 (r.a.) • Fax 011. 50.46.60
www.gruppo2g.com e-mail: gruppo2g@gruppo2g.com

30° L'IMPRESA DELLA CONOSCENZA CONTINUA 1988 • 2018

NOTIZIE

n. 026 - SETTEMBRE 2018

LA CONOSCENZA GENERA LE IDEE PER L'INNOVAZIONE DELLE IMPRESE

Aggiornamenti legislativi, normativi, tecnologici e organizzativi per migliorare il sistema di gestione aziendale

Il Manuale del Sistema di Gestione dei Dati Personali, redatto secondo BS 10012:2017, ricalca l'impostazione della nuova HLS (HIGH LEVEL STRUCTURE) che costituisce la struttura portante dei Sistemi di Gestione e che è rappresentata nello schema sottostante.

1	Scopo	Lo scopo è specifico e deve essere allineato con il contesto dell'organizzazione
2	Riferimenti normativi	Elenco di norme di riferimento altrimenti allo specifico standard.
3	Termini e Definizioni	Applicabili allo specifico standard in aggiunta a quelli comuni di tutti gli standard
4	Contesto dell'organizzazione	4.1. Comprendere l'organizzazione e il suo contesto 4.2. Comprendere le esigenze e le aspettative delle parti interessate 4.3. Determinare il campo di applicazione del Sistema di Gestione dei dati personali 4.4. Sistema di Gestione dei dati personali
5	Leadership	5.1. Leadership e impegno 5.2. Politica 5.3. Ruoli organizzativi, responsabilità e autorità
6	Pianificazione	6.1. Azioni per affrontare rischi e opportunità 6.2. Obiettivi e pianificazione del Sistema di Gestione dei dati personali per la loro realizzazione
7	Supporto	7.1. Risorse 7.2. Competenza 7.3. Consapevolezza 7.4. Comunicazione 7.5. Informazioni documentate
8	Attività operative	8.1 Pianificazione e controllo operativi
9	Valutazione delle Prestazioni	9.1. Monitoraggio, misurazione, analisi e valutazione 9.2. Audit interni 9.3. Riesame della direzione
10	Miglioramento	10.1. Non conformità e Azioni Correttive 10.2. Miglioramento continuo

5. IL RUOLO DEI CONSULENTI DEL GRUPPO 2G MANAGEMENT CONSULTING

Il Gruppo 2G Management Consulting, in questi 30 anni di attività, ha ampliato i propri servizi trasformandosi da una "società di consulenza" in una "impresa della conoscenza e di servizi innovativi" caratterizzata da una molteplicità di competenze a supporto dello sviluppo strategico delle Aziende compreso le imprese manifatturiere.

È oggi una "squadra" di 22 consulenti (in maggioranza laureati in ingegneria) che possiedono conoscenze sistemistiche e specialistiche con una predisposizione alla integrazione interdisciplinare.

La produzione ed il trasferimento della conoscenza richiede una organizzazione specifica (impresa della conoscenza) che assiste l'azienda-committente nella fase di elaborazione di dati ed informazioni esterne (andamento dei mercati, situazione socio-economica, norme, leggi, documenti contrattuali, ecc.). ed interne (risultati economici, dati progettuali, andamento produttivo, efficacia del modello organizzativo e gestionale, ecc.).

Nella nostra "impresa della conoscenza" è fondamentale il comporsi delle "fasi di produzione" in un sistema integrato poiché in termini di economia della conoscenza tutte le conoscenze richieste per arrivare al risultato sono importanti.

Per questo motivo i nostri sistemisti, esperti e specialisti operano come in una rete con un continuo scambio di dati e informazioni nonché di metodi di produzione della conoscenza. L'unità operativa è dunque rappresentata non dal singolo consulente ma dalla "filiera cognitiva nel suo insieme".

GRUPPO 2G MANAGEMENT CONSULTING

Gruppo 2G Management Consulting s.r.l.
Largo Re Umberto, 106 • 10128 - Torino Tel. 011. 50.50.62 (r.a.) • Fax 011. 50.46.60
www.gruppo2g.com e-mail: gruppo2g@gruppo2g.com

NOTIZIE
n. 026 - SETTEMBRE 2018
LA CONOSCENZA GENERA LE IDEE PER L'INNOVAZIONE DELLE IMPRESE
Aggiornamenti legislativi, normativi, tecnologici e organizzativi per migliorare il sistema di gestione aziendale

L'introduzione del Regolamento Europeo sulla protezione dei dati personali si deve integrare con gli altri obblighi organizzativi della impresa senza sovrapporsi e/o irrigidire la gestione della stessa.

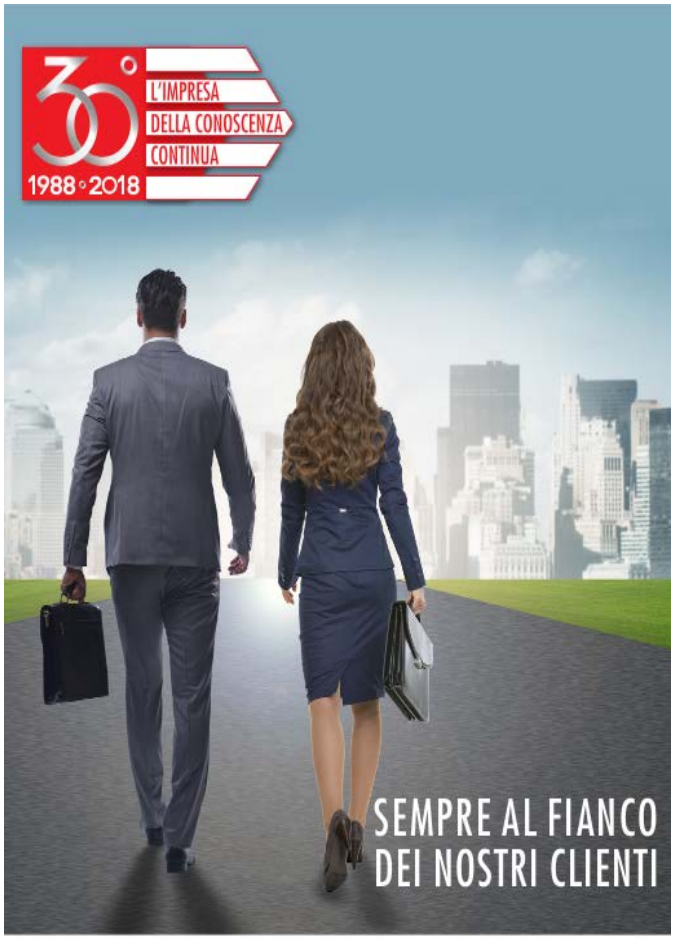
Per questo motivo è necessaria una valutazione generale dell'organizzazione aziendale finalizzata a valorizzare la prassi quotidiana e ad integrare, quando necessario e per quanto necessario, i requisiti del legislatore europeo.

L'applicazione del Regolamento Europeo sulla protezione dei dati personali si configura come una attività che richiede una visione sistemica e l'integrazione di più "conoscenze" per favorire un approccio olistico che deve operare in un contesto d'impresa che è sempre più complicato da norme, leggi e regolamenti.

Considerato che tale applicazione è valida dal 25 maggio 2018, le modifiche e integrazioni adottate con il Decreto attuativo di armonizzazione (D.Lgs 101/2018) riguardano diversi aspetti come ad esempio: gli illeciti penali e amministrativi, il consenso dei minori, la limitazione ai diritti dell'interessato, il procedimento sanzionatorio amministrativo, particolari trattamenti per ragioni di interesse pubblico, ...

In questo contesto la struttura documentale del Sistema di Gestione dei Dati Personali, nel rispetto della specificità aziendale, considererà il D.Lgs. 101/2018 che armonizza il REG. (UE) n. 679/2016.

L'attività consulenziale richiesta dell'applicazione del Reg. (UE) n. 679/2016 ha un profilo multidisciplinare con l'obiettivo di offrire all'impresa un concreto valore aggiunto trasformando quello che è considerato un peso come una opportunità imprenditoriale.



GRUPPO 2G MANAGEMENT CONSULTING

30 ANNI DI IMPEGNO PER LA PRODUZIONE DI CONOSCENZA E IL MIGLIORAMENTO CONTINUO DI SERVIZI INNOVATIVI

I Gruppo 2G Management Consulting, con il gruppo di lavoro della "GDPR", opera a supporto degli imprenditori e dei manager per affrontare e risolvere le problematiche connesse con l'adeguamento al Reg. (UE) n. 679/2016 e al D.Lgs. 101/2018 di armonizzazione del Regolamento stesso.

Per avere maggiori informazioni sulle modalità di erogazione del **SERVIZIO DI GESTIONE DEI DATI PERSONALI**
potete contattare il ns. Ufficio Marketing che fisserà un appuntamento con uno dei nostri responsabili
Ufficio Marketing: Sig.ra Cristina Gagliardo
Tel 011/505062 – Fax 011/504660
e-mail: c.gagliardo@gruppo2g.com

GRUPPO 2G MANAGEMENT CONSULTING
Gruppo 2G Management Consulting s.r.l.
Largo Re Umberto, 106 • 10128 - Torino Tel. 011. 50.50.62 (r.a.) • Fax 011. 50.46.60
www.gruppo2g.com e-mail: gruppo2g@gruppo2g.com