GRUPPO 2G

NEWS

COMPLIANCE, TECHNICAL & ORGANISATIONAL CONSULTING

009/2021

GDPR

HEALTH CHECK SUL SISTEMA DI PROTEZIONE DEI DATI E DELLE INFORMAZIONI PERSONALI

INTRODUZIONE: GDPR REG.(UE) n. 679/2016

In questi ultimi 20 anni la normativa sulla "**privacy**" ha avuto una serie di passaggi rilevanti fino ad arrivare ad oggi con **il D.Lgs. 196/03 relativo al "Codice in materia di protezione dei dati personali" novellato dal D.Lgs. 101/2019 che armonizza il Regolamento Europeo del 2016 (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 Regolamento Europeo ha una impostazione "sistemica" in cui il tema della sicurezza dei dati personali passa da una logica di "minimo" ad una logica di "adeguato" in base ai rischi che ogni Azienda deve valutare ed analizzare per decidere poi come posizionarsi.

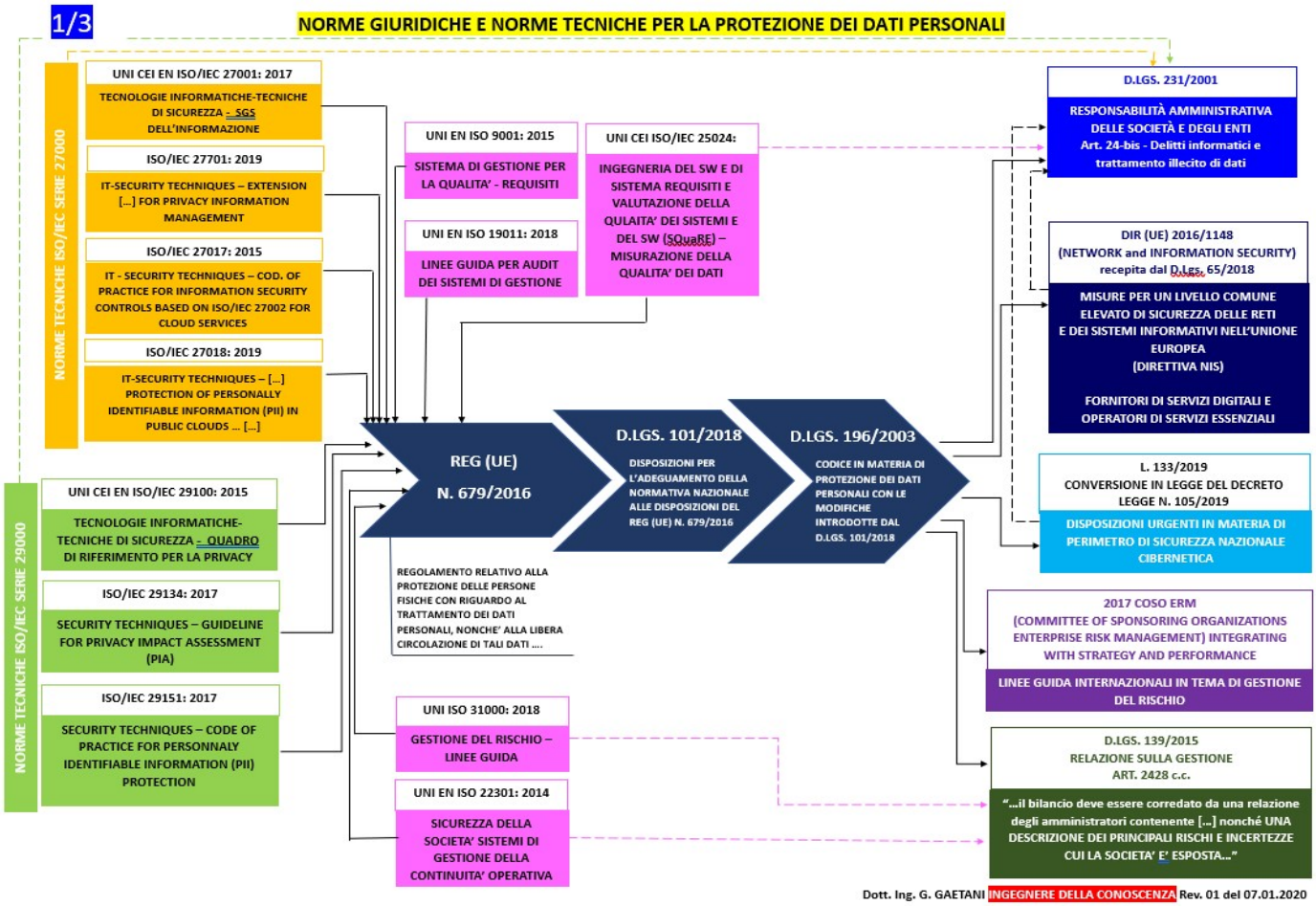
Il nuovo Regolamento Europeo sulla Privacy (GENERAL DATA PROTECTION REGULATION – GDPR) **è entrato in vigore il 24.05.2016.**

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.**

***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*. La violazione dei dati personali** (Data Breach) non sarà solo un problema confinato all'interno dell'azienda, ma **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.**

Il collegamento tra norme tecniche e giuridiche per la protezione delle persone fisiche con riguardo al trattamento dei dati personali è rappresentato sotto.



Con il Reg. (UE) n. 679/2016 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 Reg. (UE) n. 679/2016); **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).

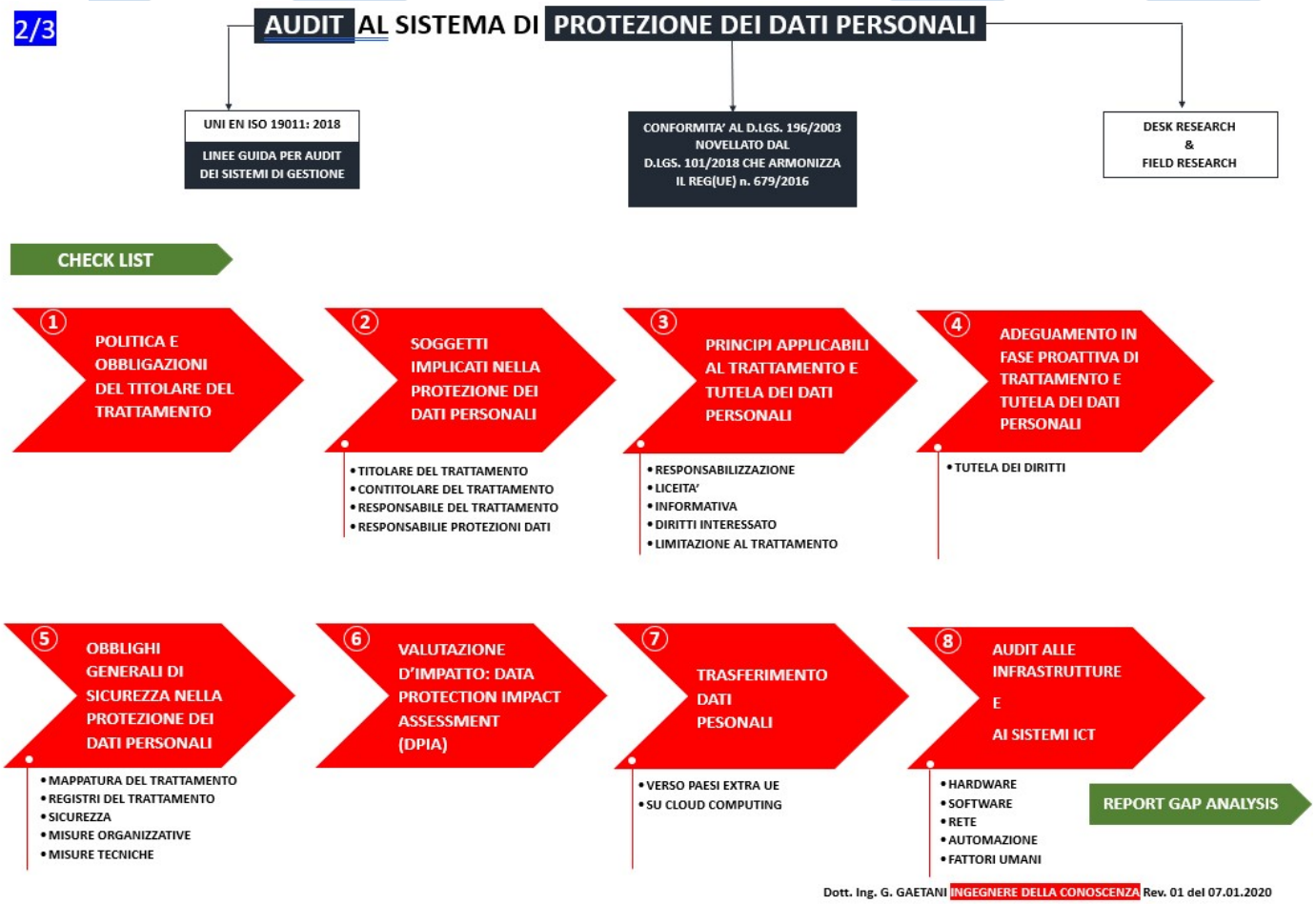
Il Reg. (UE) ha introdotto novità nell'ambito di nuove comunicazioni come la notifica in caso di rettifica, cancellazione o limitazione (art. 19), la notifica di una violazione dei dati personali all'autorità di controllo (art. 33) nonché la comunicazione di una violazione dei dati personali all'interessato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

Per quanto riguarda nuove incombenze organizzative il Reg. (UE) ha introdotto 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).

Tale certificazione 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'adesione ai […] meccanismi di certificazione approvati ai sensi dell'art. 42 …".

In questa fase è importante procedere ad un "Health Check" per verificare la consistenza del "Sistema di Gestione per la Protezione dei Dati Personali" che si può articolare, attraverso la linea guida per l'audit dei sistemi di gestione UNI EN ISO 19011:2018, alla verifica di conformità al D. Lgs. 196/03, novellato dal D. Lgs. 101/2018 che armonizza il Reg (UE) n. 679/2016.



Gruppo 2G S.p.A. - Corso Duca degli Abruzzi, 5 – 10128 – Torino Tel. 011.5620022 - www.gruppo2g.com e-mail: gruppo2g@gruppo2g.com

PROPOSTA OPERATIVA DEL GRUPPO 2G

Il Gruppo 2G S.p.A. è una "impresa della conoscenza e di servizi innovativi" che, con i suoi attuali consulenti, opera dal 1988 (33 anni!) a supporto di imprese industriali, commerciali e di servizi.

È oggi una realtà 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".
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.

Le modifiche e integrazioni adottate con il Decreto attuativo di armonizzazione (D.Lgs. 101/2018) hanno riguardato 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 dovrà essere aggiornata,** nel rispetto della specificità aziendale nonché del D.Lgs. 101/2018 che è il decreto attuativo di armonizzazione dell'ordinamento italiano al 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.

DANIELE CATASSO
- **Amministratore Delegato Gruppo 2G**
- **Esperto di Organizzazioni Aziendali Complesse, Sistemi di Controllo Interno e Risk Management**
- **Componente/Presidente di Organismi di Vigilanza ex D.Lgs. 231/2001**
- **Docente Università di Verona:**
  - **Master Internal Audit e Compliance**
  - **Corso di Perfezionamento in Frodi Aziendali: individuazione, contrasto e prevenzione**

MARCO BROVERO
- **Consulente del Gruppo 2G S.p.A.**
- **Auditor** di prima e seconda parte ai sensi della **UNI EN ISO 1901:2018**
- **Esperto in materia ambientale** e di Sicurezza secondo D.Lgs. 81/08 e smi
- **Esperto privacy (Privacy Manager)**

Per avere maggiori informazioni sui nostri servizi potete contattare il ns. Ufficio Commerciale
Sig.ra Cristina Gagliardo
che fisserà un appuntamento
con uno dei ns. responsabili.

Tel. 011.5620022
c.gagliardo@gruppo2g.com