**OGGETTO: Circolare 16.2018** **Seregno, 21 maggio 2018**

## OGGETTO: NUOVO REGOLAMENTO PRIVACY – GDPR – Note operative

Facciamo seguito alla precedente circolare n. 13 del 2 maggio 2018.

Sotto l'aspetto normativo si informa che **è stato approvato lo "schema" di decreto legislativo** (non definitivo), che introduce disposizioni per l'adeguamento della normativa nazionale al Regolamento europeo 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali**,** nonché alla libera circolazione di tali dati.

Si segnalano i seguenti interventi più rilevanti:

- il riconoscimento di un periodo transitorio di efficacia dei provvedimenti e delle autorizzazioni emanate fino ad oggi dal garante privacy.
- l'eliminazione, in materia penale, del reato connesso alla mancata adozione delle misure minime di sicurezza;
- promuovere modalità semplificate per adempiere agli obblighi in materia di privacy gravanti in capo al titolare del trattamento per le micro, piccole e medie imprese.

Sarà nostra premura portare a conoscenza del testo non appena definitivamente entrato in vigore.

Con la presente trattazione le principali procedure da attuare per **realizzare una minima attività di protezione dati per un'azienda di piccole dimensioni**. Si suggerisce di operare con questo ordine:

- Check list di base su Privacy
- Registro delle attività di trattamento (articolo 30)
- Analisi dei rischi aziendali
- Alleghiamo inoltre alcuni esempi di:
- - Informativa ex art. 13 Regolamento UE 679/2016 in materia di protezione dei dati personali
- - Atto di nomina del responsabile del trattamento dei dati

Si tralascia la definizione e la trattazione la nomina del "Responsabile della sicurezza dei dati (DPO) in quanto obbligatorio per le Pubbliche amministrazione e le aziende con oltre 250 dipendenti.

## CECK LIST DI BASE

Si ritiene analizzare e aggiornare periodicamente una check list sulle principali misure di sicurezza in azienda. Essa costituisce uno strumento sintetico di controllo per avere una immediata percezione della propria adesione alle regole sulla protezione dei dati personali e degli adempimenti che fossero eventualmente da implementare.

## REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO (ARTICOLO 30)

L'art. 30 del GDPR prescrive ai Titolari e ai Responsabili del trattamento la tenuta di un registro delle attività di trattamento svolte sotto la propria responsabilità (accountability) .
Infatti, nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici, viene affidato ai titolari il compito di decidere **autonomamente** le modalità del trattamento dei dati personali. Saranno poi i titolari stessi a dover dimostrare di aver concretamente adottato le misure finalizzate ad assicurare l'applicazione del Regolamento.

Il registro dei trattamenti, quindi, è uno **strumento fondamentale**

- per disporre di un **quadro aggiornato dei trattamenti** in essere all'interno dell'azienda
- **per ogni valutazione e analisi del rischio.**

Per questo motivo il Garante **ritiene** che *il registro dei trattamenti costituisce un adempimento* ***integrante di un sistema di corretta gestione dei dati personali***" e invita tutti i titolari del trattamento e i responsabili, a prescindere dalle dimensioni dell'organizzazione, a compiere i passi necessari per dotarsi di tale registro.

Pur non essendo un obbligo generalizzato, il registro delle operazioni di trattamento è il **punto di partenza fondamentale** per un'azienda per predisporre qualsiasi strategia in materia di protezione dei dati personali.

Il Regolamento Europeo disciplina il Registro delle Attività di Trattamento sia nel **considerando numero 82**, fondamentale per comprendere la portata dell'innovazione, che nell'**art. 30**. Esaminiamo di seguito le novità e le differenze tra questi due disposti.

Il ***considerando*** **numero 82** afferma che: *per dimostrare che si conforma al presente regolamento, il titolare del trattamento o il responsabile del trattamento dovrebbe tenere un registro delle attività di trattamento effettuate sotto la sua responsabilità. Sarebbe necessario obbligare tutti i titolari del trattamento e i responsabili del trattamento a cooperare con l'autorità di controllo e a mettere, su richiesta, detti registri a sua disposizione affinché possano servire per monitorare detti trattamenti.*
Ricordiamo che i "considerando" non sono una disposizione bensì una "motivazione dell'articolato". In questo caso si intende chiarire come l'Unione ritenga necessaria la presenza, presso ogni titolare del trattamento, di un documento ove rendicontare tutte le attività in materia di protezione e circolazione dei dati personali che lo riguardano**. La *ratio* è quella di dimostrare la conformità del titolare o del responsabile del trattamento alle disposizioni del Regolamento**.
Il considerando indica la necessità di obbligare i titolari e i responsabili del trattamento ad una collaborazione attiva con l'autorità di controllo affinché sia data dimostrazione formale e sostanziale di aver implementato tutte le misure disposte dal **Regolamento 2016/679**.

L'**art. 30 del Regolamento Europeo** approfondisce in maniera compiuta l'argomento del **considerando 82**, disponendo che:

1. ***Ogni titolare del trattamento*** *e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni:*
   *a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;*
   *b) le finalità del trattamento;*
   *c) una descrizione delle categorie di interessati e delle categorie di dati personali;*
   *d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;*
   *e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;*
   *f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;*
   *g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.*

2. ***Ogni responsabile del trattamento*** *e, ove applicabile, il suo rappresentante tengono un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento, contenente:*
   *a) il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;*
   *b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;*
   *c) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;*
   *d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.*

3. *I registri di cui ai paragrafi 1 e 2 sono tenuti in forma scritta, anche in formato elettronico.*
4. *Su richiesta, il titolare del trattamento o il responsabile del trattamento e, ove applicabile, il rappresentante del titolare del trattamento o del responsabile del trattamento mettono il registro a disposizione dell'autorità di controllo.*
5. *Gli obblighi di cui ai paragrafi 1 e 2* ***non si applicano alle imprese o organizzazioni con meno di 250 dipendenti****, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10.*

La tenuta del Registro è esclusiva del Titolare del trattamento o del suo Rappresentante (comma1 art. 30);
Come evidenziato al comma 2, anche **ogni Responsabile** del trattamento deve tenere un registro diverso rispetto a quello del Titolare/Rappresentante di cui al comma 1. Tale registro delle Attività di Trattamento del Responsabile riguarda le categorie di attività svolte per conto di un solo Titolare del trattamento con le indicazioni riportate al comma 2 sopra evidenziate.
Il comma 3 dispone come obbligatoria la **forma scritta di entrambi i Registri**.

Il comma 4 dispone che il Registro venga messo a disposizione dell'Autorità di Controllo (es. richiesta di informazioni).
Il comma 5 sancisce l'obbligatorietà del Registro delle Attività di Trattamento per tutte le grandi imprese, escludendo quindi quelle con meno di 250 dipendenti. Resta fermo che se l'impresa con meno di 250 dipendenti tratti in maniera continuativa *particolari categorie di dati personali* di cui all'art. 9 paragrafo 1, ossia i **dati sensibili**, e quelli *relativi a condanne penali e reati* di cui all'art. 10, ossia i dati giudiziari, il Registro delle Attività di Trattamento si applica pienamente.
Non viene disposto una specifica scadenza per l'aggiornamento. Si interpreta quindi che ad ogni novità riguardante gli elementi del registro corrisponda un tempestivo obbligo di aggiornamento dello stesso.
Si allega un tracciato di esempio. E' disponibile su richiesta allo Studio anche in formato in excel.

## INFORMATIVA - (ARTICOLO 13)

Il soggetto di cui tratta i dati personali (interessato), il Titolare deve fornire, prima dell'acquisizione dei dati stessi, una "**informativa" concisa, trasparente, univoca ed intellegibile** in modo da consentire al soggetto di conoscere le ragioni della richiesta.
L'informativa è un adempimento imprescindibile: occorre far sì che il soggetto cui i dati si riferiscono - l'interessato - e i cui dati stanno per entrare nelle attività dell'azienda (il suo server, i suoi computer o i suoi archivi) sia sempre informato di come quei dati saranno trattati, per quali fini, con che modi e tempi e, soprattutto, quali siano i diritti esercitabili su quei dati e nei confronti di chi.
L'informativa di cui al nuovo regolamento richiede nuove informazioni. E' maggiormente descrittiva e ai fini di rendere il trattamento ancora più trasparente, obbliga ad indicare il **periodo di conservazione** dei dati personali, l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'**accesso** ai dati personali e la **rettifica** o la **cancellazione** degli stessi o la limitazione del trattamento che lo riguardano o di **opporsi** al loro trattamento, oltre al diritto alla **portabilità** dei dati, il diritto di proporre **reclamo** a un'autorità di controllo, se la comunicazione di dati personali è un obbligo legale o contrattuale.
Si allega un fac simile di informativa.

## CONSENSO DELL'INTERESSATO (ARTICOLI 7-8)

Secondo la norma, il **consenso deve essere espresso mediante un atto positivo inequivocabile** attraverso il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile (appunto) di accettare il trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale.
Nella società tecnologica, il conferimento del consenso con simili modalità potrebbe comprendere la selezione di un'apposita casella in un sito web, o qualsiasi altra dichiarazione o comportamento che indichi chiaramente in tale contesto che l'interessato accetta il trattamento proposto.
Al contrario, non dovrebbe configurare consenso il **silenzio**, l'**inattività** o la **preselezione di caselle**.
Ci sono circostanze equivalenti al consenso, che consentono di trattare i dati personali indipendentemente dall'intervenuta acquisizione del consenso stesso. Ad esempio, il trattamento è legittimamente effettuato se necessario per l'esecuzione di un contratto di cui l'interessato è parte. Oppure quando il trattamento dei dati sia funzionale all'adempimento di un obbligo legale.

## ATTO DI NOMINA DEL RESPONSABILE DEL TRATTAMENTO DEI DATI

Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.
Il responsabile esterno è individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza;
Nell'ambito aziendale sono normalmente individuati responsabili esterni i consulenti fiscali e del lavoro.
Si allega fac simile di un atto di nomina verso lo Studio Associato Contrino quale esempio di responsabile esterno consulente fiscale.

## VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI – DPIA (ARTICOLO 35)

La valutazione d'impatto sulla protezione dei dati o DPIA (acronimo di Data Protection Inpact Assessment). consiste in **un'attività da svolgere prima di procedere al trattamento dei dati, dal titolare del trattamento**, **ogniqualvolta possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche titolari dei dati trascritti.**

Un **"rischio"** è uno scenario che descrive un evento e le sue conseguenze, stimato in termini di gravità e probabilità. La "**gestione dei rischi**", invece, può essere definita come l'insieme delle attività coordinate volte a indirizzare e controllare un'organizzazione in relazione ai rischi.
L'articolo 35 fa riferimento al possibile **rischio elevato "per i diritti e le libertà delle persone fisiche"**.
La realizzazione di una valutazione d'impatto sulla protezione dei dati è obbligatoria soltanto qualora il trattamento "possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche".

Il semplice fatto che le condizioni che comportano l'obbligo di realizzare una valutazione d'impatto sulla protezione dei dati non siano soddisfatte, non diminuisce tuttavia l'obbligo generale, cui i titolari del trattamento sono soggetti, di attuare misure volte a gestire adeguatamente i rischi per i diritti e le libertà degli interessati. In pratica, ciò significa che al fine di poter gestire i rischi per i diritti e le libertà delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. I titolari del trattamento non possono sottrarsi alla loro responsabilità coprendo i rischi stipulando polizze assicurative.

Al fine di fornire un insieme più concreto di trattamenti che richiedono una valutazione d'impatto sulla protezione dei dati in virtù del loro rischio elevato intrinseco, si forniscono i seguenti esempi.

## CASI E OBBLIGHI DI VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI – DPIA

| Esempi di trattamento | Possibili criteri pertinenti | È probabile che sia richiesta una valutazione d'impatto sulla protezione dei dati? |
|---|---|---|
| Un ospedale che tratta i dati genetici e sanitari dei propri pazienti (sistema informativo ospedaliero). | - Dati sensibili o Dati aventi carattere estremamente personale. | SI |
| | - Dati riguardanti soggetti interessati vulnerabili. | |
| | - Trattamento di Dati su larga scala. | |
| L'uso di un sistema di telecamere per monitorare il comportamento di guida sulle autostrade. Il titolare del trattamento prevede di utilizzare un sistema intelligente di analisi video per individuare le auto e riconoscere automaticamente le targhe. | - Monitoraggio sistematico. | |
| | - Uso innovativo o applicazione di soluzioni tecnologiche od organizzative. | |
| Un'azienda che monitora sistematicamente le attività dei suoi dipendenti, controllando anche la postazione di lavoro dei dipendenti, le loro attività in Internet, ecc. | - Monitoraggio sistematico. | |
| | - Dati riguardanti soggetti interessati vulnerabili. | |
| La raccolta di dati pubblici dei media sociali per la generazione di profili. | - Valutazione o assegnazione di un punteggio. | |
| | - Trattamento di Dati su larga scala. | |
| | - Creazione di corrispondenze o combinazione di insiemi di dati. | |
| | - Dati sensibili o Dati aventi carattere estremamente personale. | |
| Un'istituzione che crea una banca dati antifrode e di gestione del rating del credito a livello nazionale. | - Valutazione o assegnazione di un punteggio. | |
| | - Processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente. | |
| | - Impedisce agli interessati di esercitare un diritto o utilizzare un servizio o un contratto. | |
| | - Dati sensibili o Dati aventi carattere estremamente personale. | |
| Conservazione per finalità di archiviazione di dati sensibili personali pseudonimizzati relativi a interessati vulnerabili coinvolti in progetti di ricerca o sperimentazioni cliniche. | - Dati sensibili. | |
| | - Dati riguardanti soggetti interessati vulnerabili. | |
| | - Impedisce agli interessati di esercitare un diritto o utilizzare un servizio o un contratto. | |

| Esempi di trattamento | Possibili criteri pertinenti | È probabile che sia richiesta una valutazione d'impatto sulla protezione dei dati? |
|---|---|---|
| Un trattamento di "dati personali di pazienti o clienti da parte di un singolo medico, operatore sanitario o avvocato" (considerando 91). | - Dati sensibili o Dati aventi carattere estremamente personale. | **No** |
| | - Dati riguardanti soggetti interessati vulnerabili. | |
| Una rivista online che utilizza una lista di distribuzione per inviare una selezione quotidiana generica ai suoi abbonati. | - Trattamento di Dati su larga scala. | |
| Un sito web di commercio elettronico che visualizza annunci pubblicitari per parti di auto d'epoca che comporta una limitata profilazione basata sugli articoli visualizzati o acquistati sul proprio sito web. | - Valutazione o assegnazione di un punteggio. | |

In particolare, lo schema di decreto legislativo in esame prevede l'abrogazione di tutte quelle norme contenute nel codice privacy relative a materie che sono disciplinate da disposizioni del regolamento europeo nonché di quelle che, seppure simili alle norme europee, sono però inserite in contesti completamente diversi rispetto alle disposizioni del regolamento.

Lo Studio è in grado di assisterVi per la gestione degli adempimenti in materia di privacy e rimane a disposizione per ulteriori chiarimenti.

***Studio Commercialista Associato Contrino***