Federazione Italiana Distributori Horeca
italgrob
ASSOCIATA CONFINDUSTRIA

Roma, 3 maggio 2018

LE NUOVE NORME IN MATERIA DI PROTEZIONE DATI E L'IMPATTO SULLE IMPRESE

Ance - 23 aprile 2018

All'incontro del 23 aprile è intervenuto il prof. Francesco Pizzetti, docente di diritto costituzionale della Luiss e ex Presidente dell'autorità garante per la protezione dei dati personali dal 2005 al 2012.

Il presente approfondimento mira a sottolineare determinati aspetti del Regolamento europeo sulla protezione dei dati personali, di seguito GDPR o Regolamento, in vigore in Italia dal 25 maggio 2018, portando a riflettere sulla possibilità del GDPR di essere un vantaggio per le imprese, un investimento quasi, e non solo un costo ulteriore che grava sull'azienda.
Durante la relazione verranno portati diversi esempi pratici per favorire la maggior comprensione del contenuto del GDPR.

Premessa:
Preliminarmente si fa presente che la nuova normativa europea diverrà normativa nazionale della protezione dei dati in tutti i paesi membri dell'UE. Lo strumento del regolamento lascia agli stati membri dei margini di spazio legislativo esclusivamente per alcuni settori particolari quali la ricerca scientifica, il diritto del lavoro, la ricerca statistica e storica in quanto settori che determinano, da paese a paese, significative differenze; rimane ferma l'applicazione del GDPR anche in questi settori ma è prevista la possibilità degli stati di avere ulteriori norme più vicine, per questi settori, alla legislazione statale.
La scelta dell'utilizzo dello strumento del regolamento deriva dalla motivazione, già nel 2009 con il trattato di Lisbona, di decidere di trattare i diritti fondamentali della persona (tra cui rientra il diritto alla tutela dei dati personali), con un'unica normazione uguale per tutti i paesi UE, non potendo contrariamente essere disciplinato in modo diverso da un paese all'altro.
Al centro del GDPR c'è quindi la tutela delle persone attraverso la tutela dei loro dati personali: l'obiettivo è avere la certezza del rispetto che le informazioni che riguardano la persona siano conosciute solo da chi ha titolo per conoscerle. (es: il medico avrà delle informazioni perché deve curare il paziente, l'amministrazione ha informazioni perché il soggetto ha denunciato la nascita di un figlio, la morte di un parente, l'autosufficienza o meno di una persona per ottenere l'agevolazione sul reddito o l'assistenza sanitaria, la comunicazione della sentenza di divorzio ecc.; sono tutti dati personali che devono essere utilizzati solo per i motivi per cui vengono dati, non per altri. I dati personali quindi non riguardano solo i comportamenti che si pensa vengano spiati, ma riguardano il diritto che i dati siano utilizzati solo per il fine necessario.)
Tutto questo nell'ottica di andare sempre più in direzione della società digitale, all'interno della quale le attività economiche e le attività che ci riguardano si svolgeranno sempre di più attraverso forme di trasmissione digitale di informazioni. L'obiettivo è quello di una maggiore regolamentazione per consentire

ai cittadini di aver maggiore fiducia e non paura dei prossimi sviluppi, senza il timore di essere spiati o condizionati: è un obiettivo estremamente elevato e ambizioso ma fondamentale da raggiungere anche per lo sviluppo stesso delle imprese (es: valutare se aprire o meno un'attività commerciale in base al flusso di dati quotidiani). È importante quindi che la persona fisica sia tutelata nel momento in cui conferisce i propri dati, è questa la logica, in modo da permettere alla persona fisica di partecipare allo sviluppo della società digitale.

Premesso ciò le imprese che non si adeguano al GDPR danneggiano l'economia nazionale (es. la banca che perde i dati dei propri clienti determina un effetto a catena di mancanza di fiducia dei clienti per la banca e per il sistema italiano, portando a dubitare del servizio dell'Home banking. Quindi nessuno più delle imprese deve avere interesse a collaborare all'applicazione proattiva del regolamento, essendo una condizione essenziale per la fiducia.).

Al centro del GDPR, con la nuova impostazione data, vi è il titolare del trattamento dei dati (es. i processi attraverso i quali si usano i dati per ottenerne un risultato), non più solo l'interessato: al centro vi sono i doveri e le responsabilità del titolare. **Riassumendo al massimo, la responsabilità del titolare è quella di diminuire il più possibile il rischio del trattamento dei dati.**

Per fare cosi deve essere fatta una valutazione del rischio a monte, e non vi è più una serie di misure minime da porre in essere per tutelarsi.

Con il concetto di privacy by design si intende proprio il compito dato al titolare del trattamento di pensare e valutare fin da subito le misure necessarie per la tutela dei dati personali utilizzati in un progetto.

Per privacy by defaul invece si intende l'utilizzo minimo dei dati, solo quelli necessari; eventuali utilizzi eccessivi e non necessari devono essere segnalati e corretti.

La valutazione di impatto o di rischio deve essere sempre fatta, e consiste in un documento scritto il cui contenuto considera tutti i ragionamenti che hanno portato alle scelte effettuate dal titolare del trattamento e gli strumenti utilizzati per la protezione.

Le sanzioni:

È stato fatto molto allarmismo al riguardo. Spetta alle singole autorità di controllo stabilire quale sia la sanzione adeguata, fino ad un massimo di € 20.000.000 o il 4% del fatturato mondiale totale annuo dell'esercizio precedente. Non sono quindi sanzioni con cifra fissa, ma proporzionali al danno che si è determinato.

Il tema delle sanzioni enormi deve essere analizzato da questo punto di vista: qualsiasi azienda, anche se grande, è in proporzione nettamente più piccola rispetto alle grandi multinazionali. Quindi si vuole dare la possibilità con la sanzione di poter "spaventare" questi soggetti: devono avere un effetto rispetto all'eventuale calcolo economico di "convenienza "nel prendere una sanzione rispetto all'adeguamento della struttura.

Viene sottolineato che a volte più che la sanzione data dall'autorità può essere più preoccupante il provvedimento prescrittivo (es: l'adeguamento di tutto il sistema informatico di tutta un'organizzazione aziendale.)

Le ricadute del GDPR per le imprese:

Mettendo da parte il terrorismo che da molte società di consulenza è stato fatto nei mesi precedenti, è importante tener conto che **l'autorità di controllo non ha come mira l'obiettivo di sanzionare le imprese, quanto quello di aiutarle all'adeguamento alla nuova normativa**. Questo passaggio di visione è fondamentale.

Le imprese devono quindi iniziare a mettersi in regola, seguendo degli step precisi, mediante degli adempimenti pratici (es. tenuta del registro, adeguamento delle informative, eventuale nomina del DPO ove necessario, implementazione delle strutture di sicurezza, adeguata formazione del personale, nomine dei responsabili del trattamento).

La responsabilizzazione (accountability) è alla base del GDPR: bisogna impostare le misure adeguate alla sicurezza, non vi sono più misure minime da seguire.

È necessario nominare i responsabili esterni: tutti coloro che trattano i dati per conto del titolare.

Si specifica che ogni qual volta un soggetto esterno all'impresa è incaricato, per conto dell'impresa, di trattare i dati sulla base di un contratto o un atto giuridico (ci deve essere sempre una nomina formale, anche una convenzione, o un contratto) deve essere nominato responsabile del trattamento. (es. il servizio delle buste paga, fornitore del servizio informatico). Tutti i contratti devono quindi essere aggiornati con la nuova nomina.

Bisogna quindi iniziare a predisporre la documentazione necessaria e effettuare le nuove nomine.

La figura del DOP (Data protection officer), in particolare, è una nuova figura introdotta dal GDPR, ma non deve essere adottato da tutti: è necessario prestare particolare attenzione al riguardo. È richiesta e necessaria a seconda del tipo di trattamento dei dati che viene svolta, e dalle dimensioni di questi trattamenti. Le condizioni per la sua adozione è che si svolga un trattamento dei dati sensibili (es. dati relativi alla salute, l'orientamento sessuale, politico, religioso, ecc.) o un regolare e sistematico trattamento degli interessati su larga scala.

Deve essere una figura professionale preparata e indipendente che dialoga con l'autorità di controllo. Può essere anche un soggetto interno all'organizzazione, ma gli deve essere garantita la totale indipendenza. Deve essere un esperto di normativa sulla privacy, non un informatico, in quanto con l'autorità si discuterà e si confronterà su diritti e regole. Essendo una figura particolare non può essere rimosso dal suo ruolo se non per cause diverse dalla sua attività. Le sue decisioni non hanno effetto interdittivo, essendo l'ultima scelta spettante al titolare del trattamento, ma la sua opinione è molto influente.

I RISULTATI PRATICO OPERATIVI PER LE IMPRESE. GLI ADEMPIMENTI: IL REGISTRO, INFORMATIVE E SISTEMI DI VIDEO SORVEGLIANZA.

Di seguito una breve sintesi degli adempimenti principali che concretamente dovranno essere posti in essere.

1. **Il registro dei trattamenti**: consente di fare una mappatura di tutti i trattamenti che vengono svolti presso l'impresa dal titolare del trattamento. A livello pratico molte imprese non hanno la consapevolezza di tutti i dati e il trattamento che svolgono, come li processano, ecc.... partendo da quest'analisi invece può essere d'aiuto al titolare del trattamento per meglio gestire e organizzarsi.

Deve contenere una serie di elementi, ma il GDPR non indica poi come deve essere declinato: si stanno elaborando diversi modelli (Confindustria è in attesa del giudizio di conformità da parte del Garante Privacy del modello da lei preposto) che concretamente consisteranno in una serie di tabelle nella quale ci saranno, in primo luogo, i dati dei soggetti interessati (**titolare** -telefono, indirizzo, mail, ecc. - eventuale **contitolare** - dati del **responsabile del trattamento** con relativa indicazione dell'atto di designazione - eventuali dati del **DPO**).
Si sottolinea nuovamente l'importanza del contratto di servizio o della lettera di incarico/convenzione con cui si nomina il responsabile del trattamento (nei casi in cui i dati vengono trattati da un soggetto esterno per conto del titolare) in quanto in tal modo è possibile circoscrivere l'ambito di applicazione e le responsabilità nascenti dal GDPR.
In secondo luogo, devono essere inseriti le tipologie dei trattamenti che vengono effettuati e i processi che si vanno ad attuare. Si riportano di seguito alcuni esempi pratici:

- Gestione dei dati del personale
- Gestione dei dati dei clienti e dei fornitori
- Dati sulla formazione del personale
- Dati sulla sicurezza sul lavoro
- Dati relativi alla gestione informatica

Per tutti questi bisogna individuare la base giuridica del trattamento che può essere: il consenso dell'interessato, l'esecuzione di un contratto, un adempimento o un obbligo di legge.

Il consenso deve essere informato, quindi sempre preceduto dall'informativa, inequivocabile e consapevole per la determinata finalità indicata. Ciò comporterà che il dato ottenuto per una finalità specifica non potrà essere assolutamente utilizzato per un'altra finalità non comunicata, ma sarà necessario richiedere nuovamente il consenso dell'interessato.

2. **L'informativa:** dovrà essere inoltre chiara e comprensibile da chiunque, completa e dettagliata. Dovrà contenere il riferimento ai soggetti, titolare e responsabile del trattamento, la finalità e il tempo di conservazione, i diritti dell'interessato.

Determinate le condizioni di liceità del trattamento dovranno essere analizzate le singole voci ponendosi i seguenti interrogativi:

- Che tipologia di dati si stanno trattando?
- Sono dati personali o particolari?
- A chi sono destinati i dati?
- Chi li tratta?
- È stato nominato il responsabile/i responsabili del trattamento?
- Qual è il termine entro cui posso conservare i dati ottenuti?
- Quali misure ho messo in atto per valutare e contenere il rischio?
- Ho password, sistemi antivirus adeguati?
- Quali rischi posso correre?
- Sono stati fatti degli aggiornamenti negli ultimi tempi e sono necessarie modifiche?

3. **I sistemi di video sorveglianza**: sono ammessi, da parte del datore di lavoro, solo in presenza di alcune ragioni specifiche quali:
   - Per la salvaguardia del patrimonio aziendale.
   - Per ragioni di carattere organizzativo e produttivo.
   - Per la tutela della salute dei lavoratori.

   Pur in presenza di queste condizioni è comunque necessario ottenere dai lavoratori un consenso preventivo (dalle rappresentanze sindacali e unitarie, o in mancanza previa autorizzazione da parte dell'Ispettorato nazionale del lavoro).

   L'unica condizione per cui non è richiesto il consenso è nel caso in cui si parli di strumenti utilizzati dal lavoratore per lo svolgimento della sua mansione, ovvero nel caso in cui siano strumenti utili per la rilevazione degli accessi.