GDPR – novità e controlli

Il 25 maggio del 2018, dopo ben 2 anni è entrato in vigore il nuovo regolamento sulla privacy detto anche GDPR (General Data Protection Regulation). Il legislatore italiano in accordo con gli enti preposti al controllo del rispetto della normativa, avevano dato un anno di bonus, ovvero un periodo per "far digerire" le nuove regole alle aziende ed agli enti tenuti al rispetto del regolamento.

Ma chi sono in realtà le aziende tenute al rispetto di tali regole?

Facciamo prima a dire chi non è soggetto: i privati. Infatti il testo di legge dice che i privati nei rapporti interpersonali tra di essi non sono tenuti a tali regole.

Il bacino dei soggetti tenuti è molto ampio infatti non vi è proprio una categoria, ma per lo più una regola: **la mia azienda tratta dati personali di altri soggetti?**

Sicuramente un ente pubblico che ha a che fare ogni giorno con decine di contribuenti deve aderire al regolamento, questo è scontato. Ma per esempio: un negoziante di gioielli che fa una tessera fedeltà o una raccolta punti per i suoi clienti deve aderire? **Assolutamente si**. Il presupposto del regolamento è quello della raccolta dei dati nel vero senso della parola, il quale deve essere **lecito e trasparente**. Il **titolare del trattamento** è responsabile di tutto ciò. Questa figura in una piccola realtà imprenditoriale, solitamente è l'imprenditore stesso.

Cosa fare?
Innanzitutto dovreste domandarvi in che modo trattate i dati. Dopo di che è opportuno stilare una mappa logica dei passaggi che questi dati effettuano.
Più importante ancora: **avere una modulistica adatta all'evenienza**; sia per il regolamento, che per una vostra sicurezza, è bene avere un modulo firmato per il rilascio dei dati sottoscritto dal titolare del trattamento che dovrà spiegare in un informativa perchè sta richiedendo i dati, per quanto tempo verranno conservati e dove verranno conservati e nell'evenienza chi potrà entrare in contatto, nel caso in cui vi siano dei collaboratori.
Il punto sulla conservazione e l'ordine è molto importante, infatti in un articolo del regolamento vi è una specifica: i dati devono essere facilmente letti e verificabili dagli enti preposti al controllo. **E' utile avere una mappa logica ed un registro consultabile.**
Sul **luogo** della conservazione, non vi sono specifiche vere e proprio solo su delle note facenti riferimento ad un metodo **"ragionevole"**. Questo ci lascia intendere che non è bene tenere copie dei dati sparsi su un tavolo accessibile a tutti. Sicuramente avere un armadietto, rigorosamente chiuso a chiave, classificato e codificato sul registro interno, è un **metodo ragionevole di conservazione.**
E per l'hardware? Per chi decidesse o fosse obbligato a conservare i dati su dei supporti (PC, tablet, smartphone ecc) è bene sapere che ogni dato andrebbe copiato costantemente su un supporto esterno (HDD o un NAS), anch'essi rigorosamente protetti sia fisicamente (tenuti sotto chiave) ma anche a livello interno (password protette e difficilmente hackerabili). Le parole chiave sono: **limitare ed evitare** possibili ciber- attacchi e furti di informazioni.
Rischi? Su due fronti. Sicuramente quelli, nell'evenienza di un controllo presso la vostra azienda, di incorrere in sanzioni. Ad oggi non si sa ancora chi avrà la delega a tali verifiche, sicuramente il Garante Nazionale sulla Privacy, ma a rigor di logica la Guardia di Finanza, nell'occasione di un

controllo sporadico su un azienda. Non si escludono neanche i Carabinieri dei NAS, i quali spesso si imbattono a dei controlli in attività sanitarie: le stesse trattano dati privati di ogni genere dei loro pazienti.
Il secondo rischio che qualche vostro cliente scontento potrebbe darvi problemi legali nel caso in cui si accorga che i suoi dati non sono trattati in maniera adeguata.

Per maggiori info
http://www.studiogallarato.it/wordpress/contact-us/