DECALOGO E CODICE AZIENDALE GDPR (Regolamento UE 2016/679)

Premessa

La tutela della privacy è un diritto fondamentale e la nostra Azienda ha deciso di non affrontarlo come un obbligo burocratico convinta che adottare semplici misure a protezione dei dati personali può contribuire a rendere più efficiente l'organizzazione e a ridurre sensibilmente i potenziali rischi a cui la stessa espone sul mercato.
L'Azienda si è data questo decalogo, per dare consapevolezza a tutta la struttura e per rafforzare la capacità nel gestire al meglio i dati personali affidati, e al tempo stesso la fiducia dei clienti e del pubblico nell'affidabilità e modernità della struttura aziendale.
Il patrimonio informativo di un'azienda è un valore da tutelare e promuovere alla stregua di ogni altro asset, e può trasformarsi in una risorsa competitiva e di immagine.
Di seguito, sono indicate alcune "best practices " che compongono il decalogo che avrà come scopo quello di aiutare tutte le figure aziendali a conformarsi efficacemente alla nuova normativa.


1. 1- Categorie di Dati
2- L'Organigramma Privacy
3- Informativa e Consenso
4- Curriculm Vitae
5- Trattamenti Particolari : controllo sul lavoro
6- La tutela del patrimonio dati
7- Amministratori di Sistema
8- Trasferimenti dati all'estero
9- Diritti della Persona Interessata
10- Distruzione o perdita di dati personali

1. Categorie di dati

Siamo consapevoli che i "dati" rappresentano uno dei beni più preziosi della nostra Azienda sono di tipo commerciale, rappresentano il portafoglio degli attuali clienti o di quelli futuri, raccontano l'organizzazione interna.
Le potenzialità economiche dei dati sono direttamente proporzionali alla liceità del loro trattamento, raccogliendoli e trattandoli nel rispetto della privacy.
I dati personali sono tutte le informazioni relative a una persona fisica, identificata o identificabile, anche indirettamente (mediante riferimento a qualsiasi altra informazione), incluso l'eventuale numero di identificazione personale: sono Dati Personali , ad esempio, un indirizzo e-mail o l'immagine fotografica di una persona, il codice fiscale o un numero telefonico, un indirizzo IP o una targa automobilistica.
I dati sensibili sono quei particolari dati personali che consentono di rivelare l'origine razziale ed etnica di una persona, le sue convinzioni religiose, filosofiche o di altro genere. Lo sono anche quelli che indicano l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale. Oppure i dati idonei a rivelare lo stato di salute e la vita sessuale.
Tra i dati che necessitano di particolari cautele vi sono quelli giudiziari, una categoria che include le informazioni contenute nel casellario giudiziale e quelle connesse alla posizione di imputato o indagato in procedimenti penali, ma anche i dati biometrici o i dati genetici.

2. L'organigramma Privacy

In azienda la ripartizione dei compiti e delle responsabilità è definita con chiarezza emerge "chi fa cosa" e con quali scadenze nel rispetto del GDPR ,il nuovo Codice della Privacy ,sono definite bene quali figure hanno la possibilità di trattare dati personali.
Il titolare del trattamento è il soggetto che esercita un potere decisionale, del tutto autonomo, sulle finalità e sulle modalità del trattamento se lo ritiene utile in base all'organizzazione aziendale, può designare uno o più soggetti come responsabile del trattamento e vigila sulla puntuale osservanza delle istruzioni impartite loro.
Gli incaricati del trattamento sono le persone fisiche che effettuano le operazioni di trattamento dei dati personali e operano sotto la diretta autorità del titolare (o del responsabile se è stato nominato) secondo precise istruzioni.
Per poter svolgere queste operazioni in maniera lecita, è necessario che il personale chiamato a trattare i dati venga opportunamente designato per iscritto individuando puntualmente l'ambito di trattamento consentito e informato e formato sulle procedure aziendali per il trattamento dei dati.

3. Informativa e Consenso

L'informativa

L'Azienda spiega con attenzione agli interessati (ad esempio ai propri clienti e dipendenti), con un'informativa completa e chiara , sintetica e comprensibile, le caratteristiche essenziali dei trattamenti effettuati: dove sono stati presi i dati, le finalità e le modalità del trattamento, se i dati debbano o possano essere forniti, i soggetti o le eventuali categorie ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza, nonché il nome del Titolare e di almeno un responsabile del trattamento.

Informiamo la persona interessata prima di cominciare a utilizzare i suoi dati in maniera semplice e comprensibile :

ad esempio, ferme restando le specifiche norme di tutela previste dallo Statuto dei lavoratori, per informare le persone dell'esistenza di un sistema di videosorveglianza esponiamo dei cartelli che segnalino le telecamere e che indichino le finalità della ripresa;

Per avvisare che un veicolo aziendale è sottoposto a geolocalizzazione ,applichiamo un apposito adesivo (vetrofania) ai vetri della vettura;

In ogni caso, il trattamento aziendale dei dati è legittimo, perché il consenso dell'interessato è liberamente espresso e documentato per iscritto dopo esauriente spiegazione alla persona interessata, ad esempio un cliente, quali benefici può avere offrendo il suo assenso al trattamento dei dati.

Particolare attenzione è riservata quando si acquisiscono liste di dati personali da soggetti terzi e non direttamente dagli interessati si deve verificare sempre se gli interessati abbiano dato il proprio consenso (magari con verifiche a campione sui dati acquistati) al tipo di trattamento dati che si vuole svolgere, come quello per l'invio di offerte commerciali. L'azienda consegna l'informativa alle persone interessate già al momento della registrazione o del primo utilizzo dei loro dati..

Il consenso non è necessario quando i dati vengono trattati per adempiere, prima della conclusione di un contratto, a specifiche richieste dell'interessato, come avviene per i dati necessari per la concessione di un credito, l'emissione di una fattura, per l'esecuzione di un contratto già in essere, come quelli per la fatturazione di un prodotto o servizio.

L'Azienda richiede sempre uno specifico consenso per usare gli stessi dati per altri fini come la profilazione, lo studio dei comportamenti e delle scelte d'acquisto, il marketing in generale.

L'Azienda si impegna affinchè il cliente sia adeguatamente informato riguardo alla possibilità di opporsi in qualunque momento all'uso dei propri dati, in maniera agevole e gratuita, anche a voce o con l'invio di una e-mail, ottenendo un tempestivo riscontro dall'impresa che confermi l'interruzione delle comunicazioni commerciali e qualsiasi altro utilizzo.

Il Consenso e i dati sensibili

I dati sensibili, come le informazioni sulla salute di una persona, necessitano di tutele rafforzate. Per poterli utilizzare, l'impresa deve prima ottenere il consenso scritto della persona interessata e l'autorizzazione del Garante in casi particolari .

4. Curriculum Vitae

Nel processo di selezione del personale vi è un'attività di trattamento di dati personali dei candidati il rispetto della privacy, però, non pone limiti all'incontro della domanda di lavoro con la disponibilità dei posti offerti dalle imprese a meno che non abbiano natura sensibile (come l'appartenenza a categorie protette) o non siano destinati alla comunicazione a terzi.

L'Azienda quando avvia una selezione del personale fornisce al candidato, per iscritto, prima di acquisire il suo cv, l'informativa sul trattamento dei dati personali.

Nel caso di curriculum inviati spontaneamente nel momento in cui l'azienda decida di prendere in considerazione il curriculum e di contattare il candidato, dovrà fornire all'interessato una informativa breve con l'indicazione delle finalità e modalità del trattamento dei dati, i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati, e l'ambito di diffusione dei dati medesimi, nonché gli estremi identificativi del titolare e dell'incaricato del trattamento.

5. Trattamenti particolari: controllo sul lavoro

L'Azienda valuta con attenzione quali strumenti adottare al fine di evitare trattamenti di dati non necessari che, tra l'altro, possono risultare eccessivi o anche discriminatori.

È lecito, ad esempio, installare un sistema di videosorveglianza per esigenze organizzative e produttive, per consentire, ad esempio, di intervenire immediatamente nel caso in cui si verifichino situazioni di rischio (come negli ambienti dove si effettuano lavorazioni pericolose o rischi d'intrusione).

L'Azienda evita la raccolta di immagini che in qualche modo consentano il controllo a distanza e la verifica dell'attività dei lavoratori in osservanza delle norme previste dal Codice della privacy e quelle indicate nello Statuto dei lavoratori.

L'Azienda adotta le necessarie cautele per l'utilizzano di software che, al fine di migliorare le prestazioni della rete internet aziendale, potrebbero però consentire il monitoraggio della navigazione o della posta elettronica dei dipendenti, così come per l'utilizzo di tecnologie che consentono la precisa localizzazione del lavoratore come, ad esempio, il Gps dell'autoveicolo o dello smartphone in dotazione, o l'Rfid (Identificazione a radio frequenza) del cartellino di riconoscimento in osservanza del criteri di proporzionalità delle misure adottate.

6. La tutela del patrimonio dati

Misure minime

I dati raccolti dall'impresa rappresentano un asset fondamentale per il suo successo sul mercato. Questa necessità aziendale si trasforma in un obbligo di legge quando ad essere raccolti, conservati o trattati in qualunque modalità sono dati personali.

L'Azienda adotta idonee e preventive misure di sicurezza, in modo da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Se sono conservati in formato cartaceo l'Azienda adotta le misure di sicurezza adeguate all'armadio o alla stanza dove sono archiviati documenti e fascicoli, definisce le regole a cui devono sottostare le persone che hanno la "chiave di accesso" per accedervi e per trattarli.

Se invece sono in formato digitale, come quelli trattati attraverso computer, tablet o smartphone, l'Azienda applica tutte le misure adeguate al tipo di rischio quali la verifica dell'identità di chi accede al sistema (ad esempio, codici identificativi personalizzati, password sicure), l'adozione di un apposito sistema di autorizzazione che consenta attività predefinite, l'utilizzo di strumenti (come antivirus aggiornati e altri software e sistemi di protezione) per impedire accessi illeciti o abusivi.

Sono previste "copie di backup", in modo da poter rendere nuovamente disponibili dati e sistemi e definire misure di protezione particolari per i dati sensibili, adottando tecniche crittografiche che non li rendano immediatamente leggibili in caso di accessi illeciti.

Per la sicurezza dell'azienda e per la protezione dei dati personali, è previsto che il personale addetto a queste attività riceva un'adeguata formazione e che le misure adottate siano aggiornate.

Pur non sussistendo più l'obbligo di predisporre un "documento programmatico sulla sicurezza" che elenchi le misure adottate l'Azienda ha deciso di dotarsi di un Manuale del Proprio Sistema di Gestione Data Protection allo scopo comunque di trarre beneficio da un monitoraggio frequente della propria privacy policy e delle misure adottate per proteggere i dati, mantenendo così sotto controllo la situazione.

Misure idonee

L'Azienda è consapevole che l'adozione delle misure minime di sicurezza potrebbe risultare non sufficiente.

Il titolare, i responsabili e gli incaricati del trattamento sono consapevoli che, in caso di necessità, dovranno essere in grado di dimostrare di aver adottato tutte le misure idonee atte a ridurre i rischi connessi al non corretto utilizzo dei dati.

Cloud Computing

Particolare attenzione è prestata alla modalità con cui si adottano innovazioni tecnologiche, come quelle offerte dal cloud computing, affinché le eventuali opportunità di efficienza e risparmio non si trasformino in un rischio per la sicurezza dei dati dell'impresa.

7. Amministratori di sistema

La figura che per l'esperienza, la capacità, e l'affidabilità si occupa della gestione dei sistemi informatici e della sicurezza è l'amministratore di sistema il suo operato è trasparente e posto sotto il controllo del titolare del trattamento.
L'Azienda utilizza sistemi di controllo (presenti in tutti i moderni sistemi operativi oggi in uso) che consentano la tracciabilità degli accessi effettuati dagli amministratori di sistema agli archivi elettronici e ai sistemi di elaborazione, e la registrazione dei relativi dati per un tempo non inferiore ai sei giorni lavorativi
.
Il titolare del trattamento provvede a una verifica, con cadenza temporale definita, sulla rispondenza dell'operato degli amministratori di sistema alle misure organizzative, tecniche e di sicurezza previste dalla legge per i trattamenti di dati personali.

8. Trasferimenti di dati all'estero

Trasferimenti verso Paesi certificati
L'Azienda è consapevole che per poter "esportare" dati personali è necessario attenersi a precise regole. La normativa comunitaria prevede infatti che i dati personali possono circolare liberamente entro l'Unione europea. Per trasferire dati al di fuori dell'Unione europea devono invece essere garantiti standard di protezione adeguati a quelli europei: in caso contrario è vietato trasferire dati personali. Per semplificare l'attività di ricognizione dell'imprenditore che ha necessità di trasferire i dati, il Garante pubblica sul proprio sito internet un elenco aggiornato degli Stati "terzi" (cioè non appartenenti all'Unione europea o allo Spazio Economico Europeo) che sono già ritenuti affidabili a livello europeo e per i quali non è necessario alcun "passaporto" per l'esportazione.

Trasferimenti verso Paesi "non certificati"
Se il paese scelto non è in questa lista, l'eventuale trasferimento dei dati può essere consentito sulla base di altre garanzie adeguate che devono essere autorizzate dalle autorità europee di protezione dati, attraverso una specifica procedura che coinvolge anche il Garante italiano.
In tutti gli altri casi, valgono le eccezioni al divieto di trasferire dati in Paesi terzi: è consentito, ad esempio, il trasferimento se vi è l'apposito consenso dell'interessato (consenso scritto nel caso in cui si tratti di dati sensibili), oppure quando il trasferimento risulta necessario per l'esecuzione di obblighi derivanti da un contratto del quale è parte

l'interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato.

9. Diritti della persona interessata

Le richieste di informazione in merito al trattamento effettuato con i dati personali devono essere gestite adeguatamente, l'Azienda garantisce alla persona interessata (ad esempio dipendente, cliente o utente) specifici diritti come quello di conoscere quali siano i dati che lo riguardano in possesso dell'impresa e per quale motivo siano stati raccolti e come siano elaborati.

L'interessato può richiedere l'estrapolazione e la messa a disposizione in modo intelligibile dei dati personali, il loro aggiornamento, la rettifica o l'integrazione. In caso di violazione di legge, si può anche esigere il blocco, la cancellazione o la trasformazione in forma anonima di queste informazioni.

L'Azienda, in linea generale, garantisce che i dati personali non saranno conservati per sempre, ma solo fin quando necessario per lo scopo per il quale i dati sono stati raccolti, qualora non sia indicato per legge un preciso termine di conservazione, occorre comunque prevederlo. Una risposta puntuale e completa da parte della società è sempre un indicatore positivo di efficienza e trasparenza, oltre ad evitare un intervento del Garante da cui possano derivare provvedimenti anche sanzionatori per il mancato rispetto dei diritti dell'interessato.

10. Distruzione o perdita di dati personali

L'Azienda reagirà con prontezza ogni volta che si verifichino violazioni dei dati personali trattati in questi casi, al di là delle conseguenze in termini di responsabilità civile e penale, è opportuno avvisare gli interessati del problema riscontrato, anche per consentire loro di adottare misure che limitino i possibili pregiudizi alla persona (ad esempio, furto di identità o il danno alla reputazione) con particolare attenzione ai settori più esposti in tal senso sono quello bancario, della sanità e delle telecomunicazioni : eventuali gravi "violazioni di dati personali" subite dalle loro banche dati (le cosiddette **data breaches**) che dovessero comportare perdita, distruzione o diffusione indebita l'Azienda non solo l'obbligo di mettere in atto tutte le misure previste dal GDPR ma anche l'opportunità di dimostrare la propria efficienza e capacità di reazione.