Check-List di Analisi Preliminare GDPR

Azienda:_____

Nr. dipendenti: _____, di cui incaricati al trattamento dati: _____

- L'azienda svolge attività di marketing? _____
- L'azienda effettua controllo a distanza dei lavoratori (GPS) _____

Requisiti di Verifica	SI	NO	NOTE
Sono state individuate le categorie di dati personali trattati? informazioni che identificano o rendono identificabile una persona fisica e che possono fornire dettagli sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione i economica, ecc.			
I dati sensibili sono stati individuati e tenuti separati dagli altri dati trattati? quelli che possono rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, lo stato di salute e la vita sessuale			
I dati giudiziari sono stati individuati e tenuti separati dagli altri dati trattati? quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato.			
Sono state individuate le **finalità** di raccolta e trattamento dati personali? Se si, la base giuridica è idonea? Art 6 - liceità del trattamento: • consenso espresso • l'interessato è parte di un contratto/finalità precontrattuali • obbligo legale del titolare del trattamento • salvaguardia di interessi vitali dell'interessato • interesse pubblico/pubblici doveri • legittimo interesse del titolare			

Requisiti di Verifica	SI	NO	NOTE
Qualora il trattamento sia basato sul **consenso** dell'interessato, esso è dimostrabile? **Nb.** Per clienti e fornitori non è richiesto i consenso, ma solo l'invio dell'informativa qualora non si inviino newsletter, per le quali invece il consenso è necessario.			
La richiesta di consenso è chiara, concisa, trasparente e facilmente accessibile, con linguaggio semplice e chiaro?			
E' stato specificato che il consenso è revocabile in qualsiasi momento?			
Trattamento di categorie particolari di dati – art 9: il trattamento di dati sensibili (x es. dei dipendenti) è valido solo se (elenco non esaustivo!): • consenso espresso • resi pubblici dall'interessato • vincolato all'esecuzione di un contrato di lavoro • medicina del lavoro • professionisti soggetti al segreto professionale			
Art 12 - **L'informativa** è concisa, trasparente e facilmente accessibile, con linguaggio semplice e chiaro?			
Verificare che l'informativa contenga tutti gli elementi previsti da GDPR: • identificare titolare trattamento e DPO, se previsto • base giuridica del trattamento (se legittimo interesse, specificare qual è) • destinatari dei dati raccolti • trasferimento all'estero dei dati? • Periodo di conservazione dei dati • Diritti dell'interessato, tra cui revoca del consenso • Possibilità di reclamo al garante • Se la comunicazione dei dati è connessa all'esecuzione di un contratto, specificare le conseguenze della mancata comunicazione dei dati • Processi automatizzati e profilazione			

Requisiti di Verifica	SI	NO	NOTE
I dati sono conservati secondo un tempo non superiore a quello necessario. (eventuale procedura)			
E' definito l'ambito del trattamento (tipologia di dato e finalità) consentito agli addetti all'unità organizzativa dell'azienda? (individuazione degli incaricati e loro formazione, nonché piano di aggiornamento della formazione; regolamento interno e codice di comportamento su uso dotazioni IT)			
Il trattamento dei dati avviene secondo criteri condivisi che stabiliscono la necessità, pertinenza e completezza. (procedure interne/moduli)			
Sono state adottate misure di sicurezza tecniche e organizzative? Risultano adeguate al rischio?			
VPIA – vengono eseguiti trattamenti che possano rappresentare un rischio levato per diritti e libertà fondamentali?			Istruzioni e software del Garante disponibili
Esiste una procedura da seguire in caso di violazione dei dati (gestione del Data Breach)?			Istruzioni del Garante disponibili
Sono soddisfatti i requisiti previsti dal provvedimento del garante del 27 novembre 2008, g.u. n. 300 del 24 dicembre 2008. (AMMINISTRATORE DI SISTEMA) • Valutazione delle caratteristiche soggettive degli amministratori di sistema • Designazioni individuali degli amministratori di sistema • Elenco degli amministratori di sistema • Verifica delle attività amministratori di sistema Se il fornitori dei sistemi informativi è esterno; esso da prova di aver soddisfatto i requisiti stabiliti dal provvedimento.			

Requisiti di Verifica	SI	NO	NOTE
Se esiste un sistema di videosorveglianza che consente la visione e registrazione degli ambienti di lavoro. Si è provveduto ad ottenere opportuna autorizzazione della dtl o rappresentanze sindacali?			

NOTE: