**Allegato 4**

Oggetto: attività necessarie per l’adeguamento alle prescrizioni del regolamento UE 2016/679 (GDPR) sulla protezione dei dati personali

Allegati:

Linee Guida alla Compilazione dei Documenti

Di seguito una breve spiegazione dei contenuti dei documenti di cui alla cartella denominata “Allegato 3” che, al loro interno, contengono le note a supporto della loro compilazione.

I documenti presenti nel Kit sono ordinati in sequenza in modo da seguire l’ordine d’implementazione.

**1. Politica della Protezione dei Dati**

La Politica della Protezione dei Dati è un breve regolamento interno sulla protezione dei dati, costruito rispettando i criteri stabiliti dai codici di condotta, approvati all’Autorità del Garante della Privacy, il cui rispetto determinerà una presunzione di conformità in caso di procedimento.

Gli elementi chiave che caratterizzano questo documento sono:

* lo scopo della politica ovvero il motivo per cui viene utilizzata questa politica e perché è importante per l’azienda.
* le definizioni dei termini chiave del documento stesso come i dati personali, le categorie speciali di dati, ecc., nel contesto della Vostra organizzazione.
* i principi guida per il trattamento dei dati personali e le attività per le quali i dati personali possono essere trattati.
* i requisiti chiave che devono essere soddisfatti per essere considerati conformi alla politica e i controlli che è necessario implementare per garantire che tutte le attività di trattamento siano elencate e mappate rispetto ad ognuno degli scopi legittimi definiti nella politica.
* ruoli chiave per garantire il rispetto della Vostra politica e le responsabilità di ciascuna delle principali parti interessate come dipendenti e volontari, in modo che si sentano parte di tutto questo.
* nomina dell’autorità interne di controllo, che possono essere diverse in caso il Vostro Comitato abbia sede in più siti oltre alla specifica del modo in cui la direzione intende gestire le relazioni con le diverse autorità di controllo.

**2. Informative**

La normativa, europea e nazionale, prevede che, in base alla finalità del trattamento (ovvero il principio di finalità che stabilisce quando un trattamento di dati personali è legittimo in relazione, appunto, al fine del trattamento stesso) il Titolare dei dati del Vostro Comitato, debba fornire agli interessati (la persona fisica a cui si riferiscono i dati personali) prima del trattamento, le informazioni richieste dalle norme, attraverso il documento dell’Informativa (una comunicazione rivolta all'interessato finalizzata ad informarlo e garantirlo sulla lealtà del trattamento ovvero che i suoi dati saranno trattati per scopi determinati, espliciti e legittimi, così che possa rendere un valido consenso al trattamento dei propri dati).

Ognuno dei Vostri Comitati, dovrà rendere disponibile alle specifiche categorie di interessati – soci, dipendenti (ove presenti), fornitori, utenti-clienti - una specifica informativa.

Per i Dipendenti, l’informativa è indispensabile non solo per la fase dell’assunzione ma per tutto il periodo di gestione del rapporto lavorativo sotto il profilo previdenziale, assicurativo, fiscale, sanitario ed amministrativo in genere; ed al documento dell’informativa occorre, comunque, adempiere a prescindere se la gestione complessiva del rapporto lavorativo avviene all’interno dell’azienda o presso un professionista esterno.

**3. Lettere di autorizzazione delle figure: Titolare, Responsabile e Autorizzati**

In accordo con la normativa, ogni Comitato, dovrà identificare e nominare le figure principali relative all’attività di trattamento dei dati, all’interno della propria struttura organizzativa: il Titolare il Responsabile e gli Autorizzati.

In caso di trattamento lecito dei dati da soggetti esterni al Vostro Comitato – come ad esempio il consulente del lavoro per il trattamento dei dati dei dipendenti – sarà necessario effettuare una nomina ad hoc del professionista.

L’Autorizzato al trattamento è una figura di primissima rilevanza nell’organigramma di privacy di qualsiasi struttura poiché - sotto la diretta autorità del Titolare e del Responsabile – ogni operatore – socio o dipendente - dietro apposita autorizzazione, effettua materialmente le operazioni di trattamento sui dati personali. Nel kit è stata fornita la lettera tipo per la nomina dell’addetto all’Ufficio Legale.

**4. Atto designazione Responsabile della protezione dei Dati**

Qualora il Vostro Comitato rientri nelle ipotesi previste dall’art. 37 del Regolamento (UE) 2016/679, sarà obbligatoria la nomina del Responsabile della protezione dei dati personali (anche conosciuto con la dizione in lingua inglese data protection officer – DPO - figura prevista dall'art. 37 del Regolamento (UE) 2016/679).

Il DPO è designato dal titolare o dal responsabile del trattamento per assolvere a funzioni di supporto e controllo, consultive, formative e informative relativamente all'applicazione del Regolamento medesimo. Coopera con l'Autorità (e proprio per questo, il suo nominativo va comunicato al Garante) e costituisce il punto di contatto, anche rispetto agli interessati, per le questioni connesse al trattamento dei dati personali (artt. 38 e 39 del Regolamento).

**5. Registro dei Trattamenti**

Il **Registro dei Trattamenti** é il punto di partenza fondamentale per la conformità in materia di protezione dei dati personali.
Secondo il principio di **accountability** (responsabilità) stabilito dal Regolamento, viene affidato ai Titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati al fine di garantire un’**adeguata protezione**.

La tenuta del registro dei trattamenti è utile persino alle organizzazioni per le quali non costituisca un obbligo. A tal proposito è proprio **l’art. 30, co. 5, del GDPR ad esonerare dall’obbligo** di tenuta del registro dei trattamenti le imprese 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*”.

A conferma dell’opportunità generale di dotarsi del registro dei trattamenti, si possono considerare le raccomandazioni indicate nelle Linee Guida al regolamento, pubblicate dal Garante per la Protezione dei dati personali, in cui viene così espressamente previsto: “*la tenuta del registro dei trattamenti non costituisce un adempimento formale bensì parte integrante di un sistema di corretta gestione dei dati personali. Per tale motivo, si invitano tutti i titolari di trattamento e i responsabili, a prescindere dalle dimensioni dell’organizzazione, a compiere i passi necessari per dotarsi di tale registro e, in ogni caso, a compiere un’accurata ricognizione dei trattamenti svolti e delle rispettive caratteristiche – ove già non condotta*”.

Per quanto attiene ai soggetti obbligati alla tenuta del registro dei trattamenti, deve precisarsi che:

**L’art. 30 del GDPR**, oltre a prevedere che il registro **debba essere tenuto in forma scritta**, anche in formato elettronico e che debba essere esibito su richiesta al Garante, fornisce anche una lista di contenuti obbligatori:

* 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;

### denominazione del trattamento

* le finalità del trattamento;
* una descrizione delle categorie di interessati e delle categorie di dati personali;
* le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
* 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;
* ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
* ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all’articolo 32, paragrafo 1.

**6. Modulo di Consenso e di Recesso del Titolare della Responsabilità Genitoriale**

Tra i documenti obbligatori, il Regolamento prevede la disponibilità di questi due moduli che dovranno essere usati dal Vostro Comitato – dagli incaricati di volta in volta interessati - per ottenere il consenso ovvero per ritirarlo, da parte di un genitore / tutore legale / rappresentante di un minore al trattamento dei dati personali per uno scopo specifico.

**7. Analisi dei Rischi e Misure Adottate**

Questo documento sarà di supporto per dimostrare, in caso di controllo dalle autorità preposte, il rispetto del principio di accountability (responsabilità) stabilito dal Regolamento (artt. 5, 24) ovvero di aver seguito un percorso logico, che dimostri come si sono protette le informazioni gestite e quali rischi corrono gli interessati che autorizzano a trattare i loro dati.

Questo documento elenca quindi le minacce da cui l’organizzazione intende tutelarsi e come lo fa. Secondo l'Art. 35 del Regolamento Europeo, la valutazione di impatto contiene almeno:

* una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
* una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
* una valutazione dei rischi per i diritti e le libertà degli interessati;
* le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Nel caso in cui l’impatto non sia accettabile, va pianificata una strategia tesa a mitigare il rischio, fino a renderlo accettabile

Il documento allegato presenta questi campi:

* denominazione del trattamento
* la tipologia di dati personali e sensibili;
* Controllo, ovvero indicare se il servizio erogato comporta un monitoraggio sistematico degli spazi pubblici su larga scala;
* Disaster Ricovery, ovvero descrivi eventuali meccanismi in atto per il ripristino dei dati;
* Accesso ai dati, ovvero specificare quali persone hanno accesso ai dati personali che conservate;
* Misure di Sicurezza, ovvero elencare le misure di sicurezza messe in atto per salvaguardare i dati personali;
* Rischi identificati, facendo riferimento alla check list ISO 27001 - Sistemi di Gestione della Sicurezza delle Informazioni
* Mitigazione del Rischio, ovvero elencare le misure di protezione da implementare per mitigare i rischi identificati nel punto precedente.
* Scadenze e responsabilità per l'implementazione, indicando le date e i nomi o le funzioni delle persone responsabili dell'implementazione delle misure di protezione.
* Registrazione del completamento, indicando la data in cui le misure di protezione sono state implementate.

**8. Accordo di Riservatezza**

L'accordo di riservatezza è un contratto usato per garantire che informazioni confidenziali condivise con una controparte rimangano private e che non vengano usate per scopi diversi da quello concordato tra le parti.

**9. Registro delle Violazioni**

Il processo di risposta alle Violazione dei Dati viene avviato quando qualcuno si accorge che una sospetta / presunta o effettiva violazione dei dati personali si è verificata e lo comunica al Responsabile del Trattamento o al Titolare.

Questi documenti potrebbero essere esaminati dalle autorità di controllo, quindi devono essere scritti in modo molto preciso e accurato per garantire la tracciabilità e la responsabilizzazione.

Qualora la violazione dei dati personali o la sospetta violazione dei dati riguardasse i dati personali che vengono elaborati per conto di terzi, il Responsabile deve segnalare qualsiasi violazione dei dati personali al rispettivo Titolare dei dati senza indebito ritardo.

Nel documento viene indicato:

* La data della violazione presunta o certa;
* Una descrizione della natura della violazione
* Le categorie dei dati personali in questione
* Il numero approssimativo degli interessati
* Il nome e le informazioni di contatto del Responsabile della Protezione dei Dati
* Le conseguenze della violazione dei dati personali
* Le misure adottate per gestire la violazione dei dati personali
* Qualsiasi informazione relativa alla violazione dei dati

**10. Modello segnalazione data breach**

In caso in cui si verifichi comunque una violazione dei dati personali, nonostante le misure preventive adottate, **il titolare del trattamento ha il dovere di comunicare la violazione all’autorità di controllo** (il Garante della privacy nazionale) entro 72 ore dal momento in cui ne è venuto a conoscenza.

Nel caso in cui la stessa violazione costituisca un **pericolo per le libertà e i diritti degli interessati**, anche ad essi dovrà essere fornita adeguata comunicazione.