Lista di controllo relativa alla nuova legge sulla protezione dei dati

La seguente lista di controllo fornisce una panoramica delle misure più importanti che le associazioni dovrebbero adottare in vista dell'entrata in vigore della nuova legge sulla protezione dei dati il 1° settembre 2023. Si distingue tra le categorie «must have» (obbligatorio per legge) e «nice to have» (consigliato).

	Must have	Nice to have
Strategia di protezione dei dati		È opportuno elaborare un **piano per il raggiungimento della conformità** (preparazione dei documenti e dei processi necessari, ecc.) entro il 1° settembre 2023, che includa responsabilità, obiettivi e tempistiche.
Registro delle attività di trattamento	I titolari del trattamento devono redigere un registro di tutte le loro attività di trattamento dei dati e aggiornarlo regolarmente qualora **impieghino** almeno **250 collaboratori**. L'obbligo si applica a prescindere dal numero di collaboratori quando **i dati personali degni di particolare protezione** sono trattati **su grande scala** o se si eseguono **profilazioni ad alto rischio**.	Anche nei casi in cui la stesura di un registro non è obbligatoria, si raccomanda di stilare comunque un **inventario dei trattamenti dei dati**, considerato che qualsiasi progetto di conformità ai requisiti di protezione dei dati dovrebbe prevedere come prima cosa la determinazione delle tipologie dei dati trattati, delle modalità e delle finalità del trattamento.
Gestione del rischio relativo alla protezione dei dati	È necessario effettuare una **valutazione d'impatto sulla protezione dei dati** se il trattamento dei dati può comportare un rischio elevato per la personalità o i diritti fondamentali della persona interessata. A questo scopo sono necessari **processi di valutazione del rischio** e per l' **esecuzione di una valutazione d'impatto sulla protezione dei dati**.	

	Must have	Nice to have
Obbligo di informare le persone interessate	Quando si raccolgono dati personali, la persona interessata deve essere **informata del trattamento previsto**. L'attività d'informazione deve far sì che la persona interessata riceva tutte le informazioni necessarie per esercitare i propri diritti e garantire un trattamento trasparente dei dati.	Le informazioni non devono necessariamente essere fornite per iscritto. Tuttavia, si raccomanda vivamente di farlo per motivi probatori e pratici. L'obbligo di informare viene solitamente adempiuto mediante la presentazione di una **dichiarazione sulla protezione dei dati**, ad esempio nell'ambito del processo di registrazione come membro dell'associazione, sul sito Web, nei rapporti con il personale.
Regolamenti/direttive interni	In determinate circostanze sussiste l'obbligo di tenere un **registro** dei trattamenti dei dati e di redigere un **regolamento sul trattamento**, in particolare se viene effettuato un trattamento automatizzato di dati personali degni di particolare protezione su ampia scala o se viene effettuata una profilazione ad alto rischio.	A prescindere da questi eventuali obblighi, è opportuno redigere **una direttiva interna** con **istruzioni** per i dirigenti e i collaboratori dell'associazione sulle procedure di gestione dei dati personali e della sicurezza delle informazioni, al fine di garantire la conformità alle norme sulla protezione dei dati. All'interno della direttiva è anche possibile definire le **responsabilità e i ruoli** interni in materia di protezione dei dati.
Trattamento dei dati da parte di terzi	Se il **trattamento dei dati viene affidato a parti terze esterne** (ad esempio, a una società informatica che ospita il sito Web dell'associazione e, di conseguenza, ha accesso ai dati personali), è necessario garantire che tali **parti terze trattino** i **dati personali con le medesime modalità consentite al titolare del trattamento** e siano in grado di garantire la **sicurezza dei dati**.	Per motivi probatori e pratici, è opportuno stipulare con la parte terza un **contratto di nomina a responsabile del trattamento dei dati personali**, all'interno del quale vengono definiti i diritti e gli obblighi tra il titolare del trattamento e il responsabile del trattamento.

	Must have	Nice to have
Regolamento sugli obblighi di conservazione e cancellazione	Il principio della **limitazione delle finalità** prescrive che i dati personali vengano trattati solo per le finalità specificate al momento della raccolta, prescritte per legge o dettate dalle circostanze. Di conseguenza, **in linea di principio i dati** devono **essere cancellati una volta raggiunto lo scopo** (ad esempio, quando un membro esce dall'associazione), fatti salvi eventuali **obblighi di conservazione** per periodi più lunghi (ad esempio, 10 anni per i documenti contabili) o altri motivi giustificativi.	Si raccomanda di redigere un **regolamento interno** sugli obblighi relativi alla conservazione e alla cancellazione dei dati personali. Questo può anche essere integrato nella direttiva interna di cui sopra.
Sicurezza dei dati	I titolari del trattamento dei dati devono garantire una sicurezza dei dati adeguata al rischio, implementando **misure tecniche e organizzative** (MTO) adeguate.	Si raccomanda di **specificare** le **MTO per iscritto**.
	In caso di **incidente di sicurezza dei dati** (ad esempio se i dati personali vengono involontariamente divulgati o resi accessibili a soggetti non autorizzati), qualora il rischio sia elevato è necessario informare l'IFPDT il più rapidamente possibile. La persona interessata deve essere informata qualora ciò sia necessario per la sua protezione.	Può essere opportuno redigere una **procedura scritta** per la valutazione del rischio di un incidente di sicurezza dei dati e per l'eventuale notifica all'IFPDT e alla persona interessata, comprese le istruzioni operative e le responsabilità.

	Must have	Nice to have
Diritti degli interessati	**Diritto all'informazione**: la persona interessata può richiedere informazioni sul trattamento dei dati personali che la riguardano. L'associazione deve essere in grado di fornire le informazioni richieste.	Laddove opportuno è opportuno definire una **procedura scritta** per la gestione delle richieste e delle domande a questo riguardo, in cui siano contenute le necessarie istruzioni operative e responsabilità. Nell'ambito del principio di esattezza, si raccomanda inoltre di introdurre un processo di **controllo periodico** dei dati personali trattati dall'associazione.
	Diritto di rettifica: la persona interessata può richiedere la rettifica dei dati personali errati. L'associazione deve essere in grado di correggere i dati.	
	Portabilità dei dati: la persona interessata può richiedere al titolare del trattamento di ricevere i dati personali che ha fornito al titolare del trattamento e che quest'ultimo ha elaborato automaticamente. L'associazione deve essere in grado di fornire alla persona interessata i suoi dati in un formato elettronico di uso comune o di trasferirli, su richiesta, a un altro titolare del trattamento.	
Trasferimenti di dati all'estero	Se **i dati** vengono **trasferiti all'estero**, il titolare del trattamento deve garantire la protezione dei dati, anche nel caso in cui un responsabile del trattamento abbia **accesso dall'estero ai dati personali** dell'associazione. In particolare, se i dati vengono trasferiti verso un paese destinatario in cui non viene garantito un **livello adeguato di protezione dei dati** (ad esempio, verso gli Stati Uniti), devono essere fornite **garanzie** aggiuntive (ad esempio, clausole standard di protezione dei dati) e, prima del trasferimento, deve essere effettuata una **valutazione dell'impatto del trasferimento dei dati**.	Si raccomanda di definire per **iscritto** il processo di valutazione del Paese destinatario e l'introduzione di eventuali garanzie e misure aggiuntive, comprese le istruzioni operative e le responsabilità.

	Must have	Nice to have
Sensibilizzazione e formazione sulla protezione dei dati		L'attuazione e il rispetto delle norme sulla protezione dei dati e delle direttive interne richiede un'adeguata consapevolezza all'interno dell'associazione. Di conseguenza, si raccomanda di organizzare **corsi di formazione** periodici sulla **protezione dei dati**.
Consulente per la protezione dei dati		La nomina di un **consulente** (interno o esterno) **per la protezione dei dati**, i cui dati di contatto devono essere comunicati all'IFPDT, non è obbligatoria, ma può essere utile.
Revisione regolare delle misure di protezione dei dati		Si raccomanda di **rivedere e aggiornare regolarmente** le misure di protezione dei dati e la relativa **osservanza**.